TRANSMISSION BASICS AND NETWORKING MEDIA

After reading this chapter and completing the exercises, you will be able to:

- Explain data transmission concepts including full-duplexing, attenuation, and noise
- Describe the physical characteristics of coaxial cable, STP, UTP, and fiber-optic media
- Compare the benefits and limitations of different networking media
- Identify the best practices for cabling buildings and work areas
- Describe methods of transmitting data through the atmosphere

ON THE JOB

I was once asked to test the quality of various network-monitoring software packages. Our test lab had all the latest new equipment to mimic the client's LAN: managed stacks of 100-MHz hubs, powerful Intel-based servers with RAID subsystems, and nicely configured workstations. We also had the best surge arrestors available and an excellent UPS system.

Installation of the operating systems went well, but the results from the various management programs were unreliable. It soon became apparent that the lab contained bad hardware; the logs of traffic on the server NICs showed too many errors for a busy LAN—let alone an isolated test LAN. Internal diagnostics programs said that the cards were okay. When I generated as much traffic as I could through the new hubs, using a laptop with a new NIC, I found no errors.

What was next? I had checked the system's entire Physical layer—except for the LAN's wires. When testing the hubs, I had used the new cable that came with my new NIC. I visually double-checked the termination patterns to verify that I had a proper TIA-568 CAT5 cable. A continuity test also showed the cables to be correct.

Finally, I decided to reterminate the cable ends. As soon as I snipped off the ends and exposed the wires, it became apparent that the cable was CAT3 at best! In fact, our company was color-coding cables, using one color for one purpose. It had ordered several large spools from the same vendor—but the vendor did not check the wire before shipping it. The green twisted-pair cable used for my project was not stamped with a CAT5 verification and was not of the same quality as the other cable in the shipment.

Quality cable is as critical as quality memory or RAID subsystems. Termination of cable can be poorly done, however, leading to intermittent, difficult-to-trace problems. As little as 1 inch of untwisted wire at cable ends can reduce the capacity of a wire set from 150 MHz to 30 MHz! In my case, a CAT5 test on a high-quality cable tester would have detected the cable problem. I've learned my lesson. When odd problems arise on high-speed connections, I head for our company's sophisticated cable and fiber tester.

Tom Callaci

Berbee Information Networks, Inc.

Just as highways and streets provide the foundation for automobile travel, networking media provide the physical foundation of data transmission. As you know, networking media reside at the lowest layer of the OSI Model. The first networks transmitted data over thick, heavy coaxial cables.

Today, most networking media resemble telephone cords, with their flexible outsides and twisted copper wire inside. Because networks now demand more speed, versatility, and reliability, however, networking media are changing. Modern networks may incorporate not only copper wiring, but also fiber-optic cables, infrared, radio waves, and possibly other media.

Before you can fully understand network communications, you must understand how data are transmitted. You should also be familiar with the characteristics of various networking media. Although network users take data transmission for granted, giving little thought to how their e-mail messages or files move from point A to point B, you need to understand this process thoroughly. This chapter discusses the details of data transmission. You'll learn what it takes to make data transmission dependable and how to correct some common transmission problems.

Transmission Basics

In data networking, the term **transmission** has two meanings. First, it can refer to the process of issuing data signals on a medium. It can also refer to the progress of data signals over a medium from one point to another. Long ago, people transmitted information across distances via smoke or fire signals. Needless to say, many different types of data transmission have evolved since that time. The transmission techniques in use on today's networks are complex and varied. In the following sections you will learn about some fundamental characteristics that define today's data transmission. In later chapters you will learn about more subtle and specific differences between types of data transmission.

Analog and Digital Signaling

One important characteristic of data transmission is the type of signaling involved. On a data network, information can be transmitted via one of two signaling methods: analog or digital. Both types of signals are generated by electrical current, the pressure of which is measured in **volts**. The strength of an electrical signal is directly proportional to its voltage. Thus, when network engineers talk about the strength of an analog or digital signal, they often refer to the signal's **voltage**.

The essential difference between analog and digital signals is the way voltage creates and sustains the signal. In **analog** signals, voltage varies continuously. In **digital** signals, voltage turns off and on repeatedly, pulsing from zero voltage to a specific positive voltage. An analog signal's voltage appears as a continuous wave when graphed over time, as shown in Figure 4-1.

Because voltage is varied and imprecise in analog signals, analog transmission is more susceptible to transmission flaws such as noise (discussed later) than digital signals. To understand this concept, think of two tin cans connected by a wire. When you speak into one of the tin cans, you produce analog sound waves that vibrate over the wire until they reach the tin can at the other end. These sound waves are merely approximations of your voice, and they are significantly affected by the quality of the wire. For example, if you try the tin can experiment with a pure copper wire, your voice will arrive at the other end sounding clearer than if you used fishing line, because copper conducts sound better than plastic. Regardless of which medium you use, however, the sound waves will become distorted as they traverse the wire, arriving at the second tin can at least a little muddled. This vulnerability makes analog transmission less precise than digital transmission.

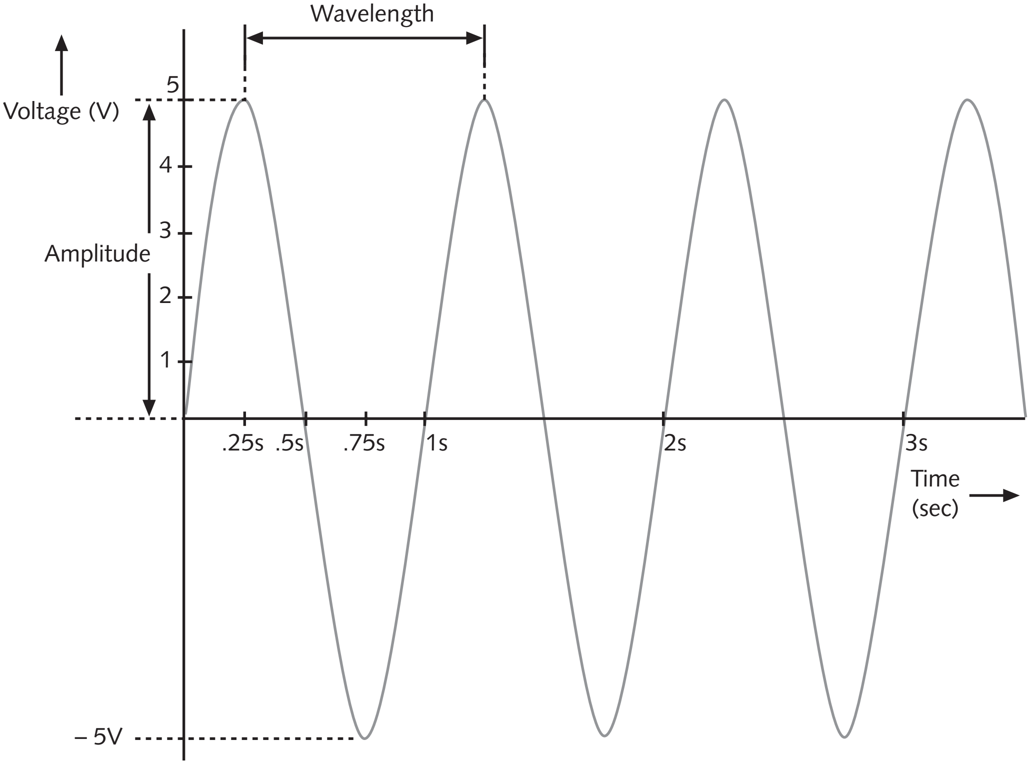

Figure 4-1 An example of an analog signal

An analog signal, like other waveforms, is characterized by four fundamental properties: amplitude, frequency, wavelength, and phase. A wave's **amplitude** is a measure of its strength at any given point in time. On a wave graph, the amplitude is essentially the height of the wave. In Figure 4-1, for example, the wave has an amplitude of 5 volts at .25 seconds and an amplitude of 0 volts at .5 seconds, and an amplitude of –5 volts at .75 seconds.

Whereas amplitude indicates an analog signal's strength, **frequency** is the number of times that a signal's amplitude cycles from its starting point to its highest or lowest amplitude, then to its lowest or highest amplitude and back to its starting amplitude over a fixed period of time. Frequency is expressed in cycles per second, or **hertz (Hz)**, named after German physicist Heinrich Hertz, who experimented with electromagnetic waves in the late nineteenth century. For example, in Figure 4-1 the wave cycles to its highest then lowest amplitude and returns to its starting point once in 1 second. Thus, the frequency of that wave would be 1 cycle per second, or 1 Hz—which, as it turns out, is an extremely low frequency. Frequencies used to convey speech over telephone wires fall in the 300 to 3300 Hz range. An FM radio station may use a frequency between 850,000 Hz (or 850 KHz) and 108,000,000 Hz (or 108 MHz) to transmit its signal through the air. You will learn more about radio frequencies used in networking later in this chapter.

The distance between corresponding points on a wave's cycle is called its **wavelength**, as shown in Figure 4-1. Wavelengths are expressed in meters or feet. A wave's wavelength is inversely proportional to its frequency. In other words, the higher the frequency, the shorter the wavelength. For example, a wave with a frequency of 1,000,000 cycles per second (1MHz) has a wavelength of 300 meters, while a wave with a frequency of 2,000,000 Hz (2 MHz) has a wavelength of 150 meters.

The term **phase** refers to the progress of a wave over time in relationship to a fixed point. An analogy will help to clarify this concept. Imagine that you and a friend are walking on the beach, both of you dragging a stick through the sand, swinging it from right to left in a wave pattern. Assume that both of you swing your sticks the same distance to the right and left (amplitude), and also assume that you are walking at the same rate (frequency). If you and your friend begin at the same spot, your waves will have equivalent phases. If, however, your friend starts one foot in front of you, even though she is dragging her stick the same distance to the left and right and walking at the same pace, your waves will not look identical because their maximum heights will not line up. That is, their phases will differ. Figure 4-2 illustrates the concept of phase.

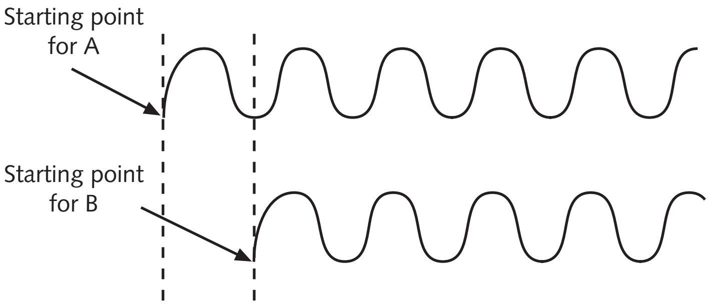

Figure 4-2 Phase differences

So far you have learned about wave properties applied to a very simple, single-frequency wave. However, voices and instruments emit a complex composite of fundamental tones whose frequencies and amplitudes rapidly vary. Figure 4-3 provides an example of an analog signal of a person speaking a full sentence. Because each person's voice patterns vary, a representation of the signal you generate when speaking the same sentence would look somewhat different.

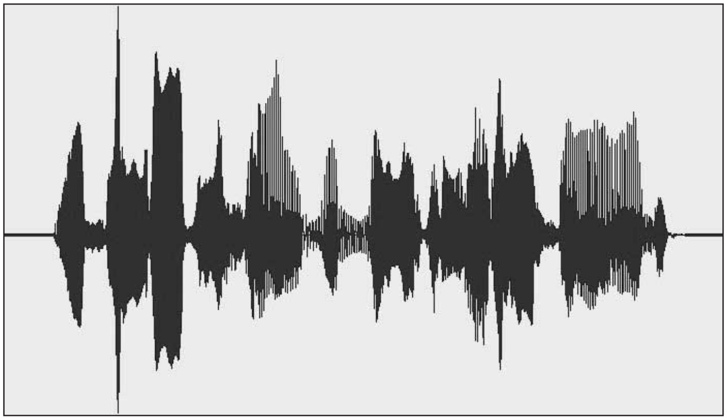

Figure 4-3 A complex analog signal representing human speech

One benefit to analog signals is that, because they are more variable than digital signals, they can convey greater subtleties. For example, think of the difference between your voice and the digital voice of an automated teller machine or a digital answering machine. These digital voices have a poorer quality than your own voice—that is, they sound "like machines." They can't convey the subtle changes in inflection that you expect in a human voice.

Now contrast the analog signals pictured in Figures 4-1 through 4-3 to a digital signal, as shown in Figure 4-4. Digital signals are composed of pulses of precise, positive voltages and zero voltages. A pulse of positive voltage represents a 1. A pulse of zero voltage (in other words, the lack of any voltage) represents a 0. As in any **binary** system, these 1s and 0s combine to encode information. Every pulse in the digital signal is called a binary digit, or **bit**. A bit can have only one of two possible values: 1 or 0. Eight bits together form a **byte**. In broad terms, one byte carries one piece of information. For example, the byte "01111001" means "121" on a digital network. As you learned in Chapter 3, in the case of TCP/IP addressing, a byte is also known as an octet.

Because digital transmission involves sending and receiving only a pattern of 1s and 0s, represented by precise pulses, it is more reliable than analog transmission, which relies on variable waves. In addition, **noise**, or any type of interference that may degrade a signal affects digital transmission less severely. On the other hand, digital transmission requires many pulses to transmit the same amount of information that an analog signal can transmit with a single wave. For example, you might convey the word "one" with a few waves in analog format; in digital format, however, the same message would require 8 bits (00000001), or eight separate pulses. Nevertheless, the high reliability of digital transmission makes this extra signaling worthwhile. In the end, digital transmission is more efficient than analog transmission, because it causes fewer errors and, therefore, requires less overhead to compensate for errors.

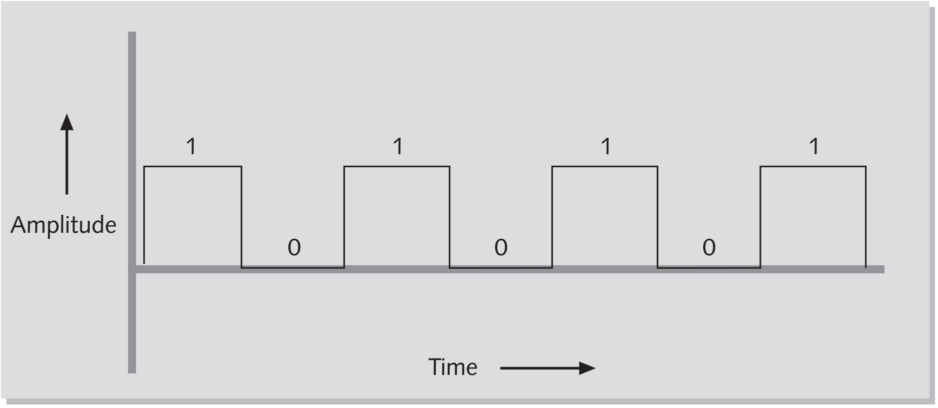

Figure 4-4 An example of a digital signal

Note

Overhead is a term used by networking professionals to describe the nondata information that must accompany data in order for a signal to be properly routed and interpreted by the network. Overhead is also used in other professions to describe what must be done in addition to a stated task in order to accomplish that task. For example, suppose you want a loan from your bank. The task you wish to accomplish is simply obtaining a certain amount of money. However, you must first talk with a bank employee and complete an application. The bank employee then must run a credit check to make sure you are a safe risk. The credit check may require the cooperation of other financial institutions. If the loan is very large, it may require the involvement of other bank employees. After more paperwork, and a review process, the loan will be approved. Next the bank will issue you a check. Its employees will also update your personal account information. Most of these steps do not equal giving you money. Instead, they contribute to the overhead of obtaining money. Data transmission overhead is an important networking concept when analyzing a network's performance, because, when all other factors are equal, the more overhead a transmission requires, the longer it will take to reach its destination.

It is important to understand that in both the analog and digital worlds, a variety of signaling techniques are used. For each different technique, standards (established by professional organizations such as IEEE or government organizations such as the FCC) dictate what type of transmitter, communications channel, and receiver should be used. For example, the type of transmitter (NIC) used for computers on a LAN and the way in which this transmitter manipulates electric current to produce signals is different from the transmitter and signaling techniques used on a satellite dish. While not all signaling methods are covered in this book, you will learn about the most common methods used for data networking.

Data Modulation

Most networks rely exclusively on digital transmissions. One situation in which you are likely to employ analog signals to transmit data is when you use a modem to connect two systems. The modem may transmit signals in analog over the phone lines, but the signals must be converted into digital signals by the modem at the receiving computer. The word **modem** reflects this device's function as a *mod*ulator/*dem*odulator—that is, it modulates digital signals into analog signals at the transmitting end, then demodulates analog signals into digital signals at the receiving end. (You will learn more about modem communications in Chapter 7.)

Data modulation is a technology used to modify analog signals in order to make them suitable for carrying data over a communication path. In **modulation**, a simple wave, called a carrier wave, is combined with another analog signal to produce a unique signal that gets transmitted from one node to another. The carrier wave has preset properties (including frequency, amplitude, and phase). Its purpose is merely to help convey information; in other words, it does not represent information. Another signal, known as the information or data wave, is added to the carrier wave. When the information wave is added, it modifies one property of the carrier wave (for example, the frequency, amplitude, or phase). The result is a new, blended signal that contains properties of both the carrier wave and added data. When the signal reaches its destination, the receiver separates the data from the carrier wave.

Modulation can be used to make a signal conform to a specific pathway, as in the case of **frequency modulation (FM)** radio, in which the data must travel along a particular frequency. Modulation may also be used to issue multiple signals to the same communications channel and prevent the signals from interfering with one another. In frequency modulation, the frequency of the carrier signal is modified by the application of the data signal. Figure 4-5 depicts an unaltered carrier wave, a data wave, and the combined wave as modified through frequency modulation. (In **amplitude modulation (AM)**, the amplitude of the carrier signal is modified by the application of the data signal.) Later in this book you will learn about networking technologies, such as DSL, that make use of modulation.

Transmission Direction

Data transmission, whether analog or digital, may also be characterized by the direction in which the signals travel over the media.

Simplex, Half-Duplex and Duplex

In cases where signals may travel in only one direction, the transmission is considered **simplex**. For example, a football coach calling out orders to his team through a megaphone is using simplex communication. In this example, the coach's voice is the signal, and it travels in only one direction—away from the megaphone's mouthpiece and toward the team. Simplex is sometimes called one-way, or unidirectional, communication.

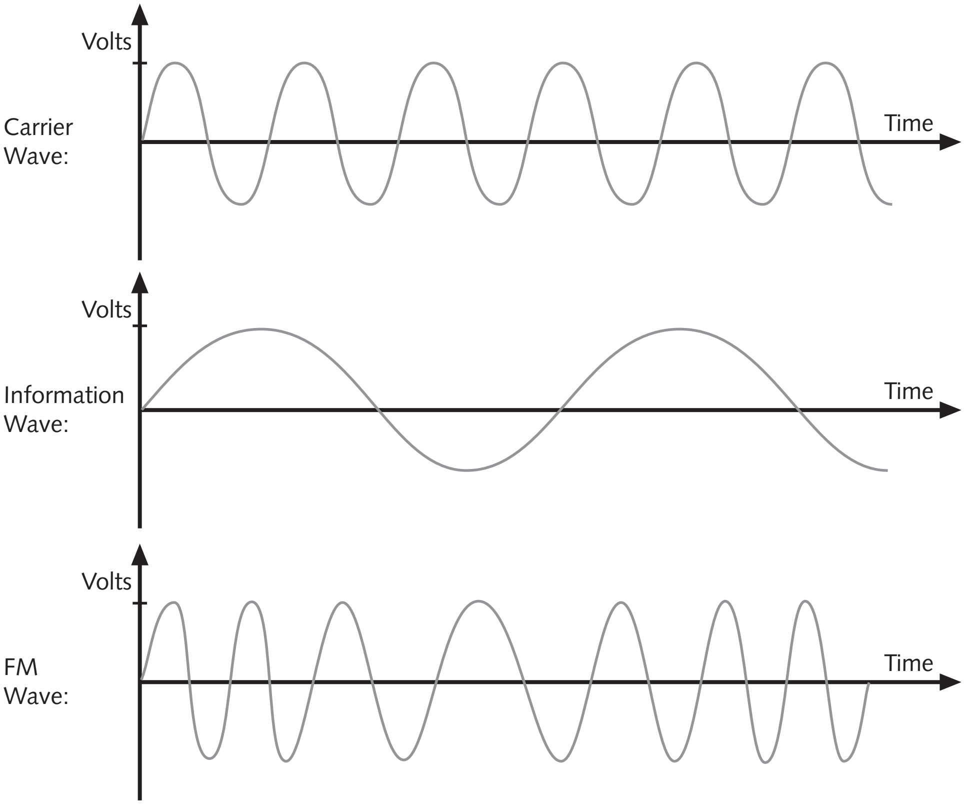

Figure 4-5 A carrier wave modified by frequency modulation

In **half-duplex** transmission signals may travel in both directions over a medium but in only one direction at a time. Half-duplex systems contain only one channel for communication, and that channel must be shared for multiple nodes to exchange information. For example, an apartment's intercom system that requires you to press a "talk" button in order to allow your voice to be transmitted over the wire uses half-duplex transmission. If you visit a friend's apartment building, you press the "talk" button to send your voice signals to their apartment. When your friend responds, he presses the "talk" button in his apartment to send his voice signal in the opposite direction over the wire to the speaker in the lobby where you wait. If you press the "talk" button while he's talking, you will not be able to hear his voice transmission. In a similar manner, some networks operate with only half-duplex capability over their wires.

When signals are free to travel in both directions over a medium simultaneously, the transmission is considered **full-duplex**. Full-duplex may also be called bidirectional transmission or sometimes, simply **duplex**. When you call a friend on the telephone, your connection is an example of a full-duplex transmission, because your voice signals can be transmitted to your friend at the same time your friend's voice signals are transmitted in the opposite direction to you. In other words, both of you can talk and hear each other simultaneously.

Full-duplex transmission is also used on data networks. For example, modern Ethernet networks use full-duplex. In this situation, full-duplex transmission uses multiple channels on the same medium. A **channel** is a distinct communication path between two or more nodes, much as a lane is a distinct transportation path on a freeway. Channels may be separated either logically or physically. You will learn about logically separate channels in the next section. An example of physically separate channels occurs when one wire within a network cable is be used for transmission while another wire is used for reception. In this example, while each separate wire in the medium allows half-duplex transmission, when combined in a cable they form a medium that provides full-duplex transmission. Full-duplex capability increases the speed with which data can travel over a network. In some cases—for example, telephone service over the Internet—full-duplex data networks are a requirement. Figure 4-6 compares simplex, half-duplex, and full-duplex transmissions.

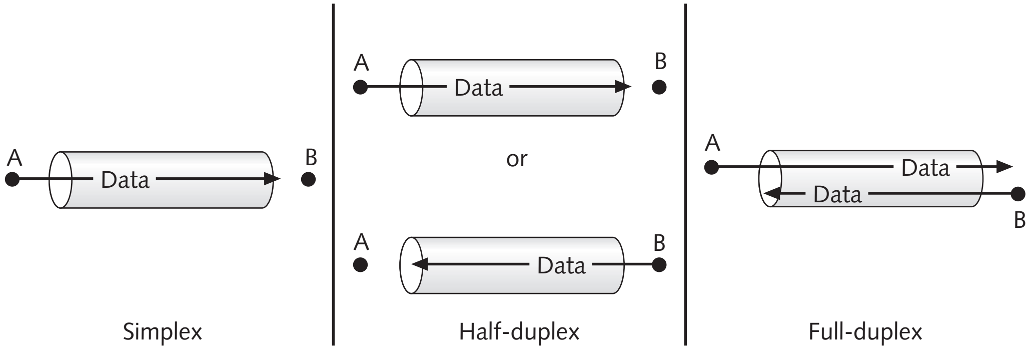

Figure 4-6 Simplex, half-duplex, and full-duplex transmission

Many network devices, such as modems and NICs, allow you to specify whether the device should use half- or full-duplex communication. It's important to know what type of transmission a network supports before installing network devices on that network. If you configure a computer's NIC to use full-duplex while the rest of the network is using half-duplex, for example, that computer will not be able to communicate on the network. Network hardware settings are explained in more detail in Chapter 6.

Multiplexing

A form of transmission that allows multiple signals to travel simultaneously over one medium is known as **multiplexing**. In order to accommodate multiple signals, the single medium is logically separated into multiple channels, or **subchannels**. There are many different types of multiplexing, and the type used in any given situation depends on what the media, transmission and reception equipment can handle. For each type of multiplexing, a device that can combine many signals on a channel, a **multiplexer (mux)**, is required at the sending end of the channel. At the receiving end, a **demultiplexer (demux)** separates the combined signals and regenerates them in their original form.

Multiplexing is commonly used on networks to increase the amount of data that can be transmitted in a given time span. For example, one type of multiplexing, **time division multiplexing (TDM)**, divides a channel into multiple intervals of time, or time slots. It then assigns a separate time slot to every node on the network and in that time slot, carries data from that node. For example, if five stations are connected to a network over one wire, five different time slots would be established in the communications channel. Workstation A may be assigned time slot 1, workstation B time slot 2, workstation C time slot 3, and so on. Time slots are reserved for their designated nodes no matter whether the node has data to transmit or not. If a node does not have data to send, nothing will be sent during its time slot. This arrangement can be inefficient if some nodes on the network rarely send data. Figure 4-7 shows a simple TDM model.

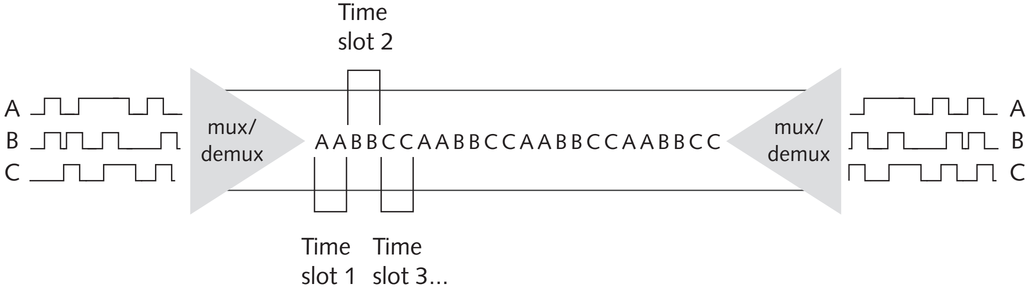

Figure 4-7 Time division multiplexing

Statistical multiplexing is similar to time division multiplexing, but rather than assigning a separate slot to each node in succession, it assigns slots to nodes according to priority and need. This method is more efficient than TDM because in statistical multiplexing time slots are unlikely to remain empty. To begin with, statistical multiplexing, like TDM, assigns one time slot per node. However, if a node doesn't use its time slot, statistical multiplexing devices will recognize that and assign its slot to another node that needs to send data. The contention for slots may be arbitrated according to use or priority or even more sophisticated factors, depending on the network. Most importantly, statistical multiplexing allows networks to maximize available bandwidth. Figure 4-8 depicts a simple statistical multiplexing system.

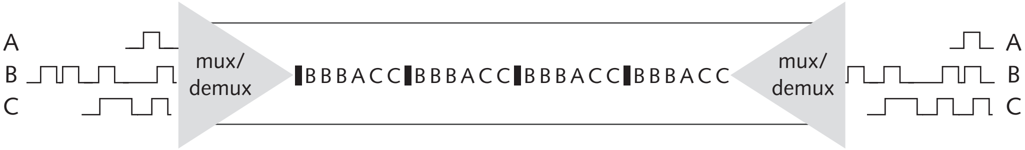

Figure 4-8 Statistical multiplexing

Wavelength division multiplexing (WDM) is a relatively new technology used only with fiber-optic cable. In fiber-optic transmission, data is represented as pulses of light (you will learn more about how this occurs later in this chapter). WDM enables one fiber-optic connection to carry multiple light signals simultaneously. Each carrier signal in WDM is assigned a different wavelength, which equates to its own separate subchannel. The wavelength of each carrier signal is then modulated with a data signal. In this manner multiple signals can be simultaneously transmitted in the same direction over a length of fiber. In fact, using WDM, a single fiber can transmit as many as 2 million telephone conversations.

Depending on the type of equipment and fiber used, WDM may send multiplexed signals in one direction or two directions simultaneously. At the transmitting end, an WDM wave is created by a **fiber-optic modem (FOM)** and at the receiving end, an FOM separates the multiplexed signals into individual signals according to their different wavelengths, as shown in Figure 4-9. In between, the multiple signals may need to be regenerated to carry over long distances, but with lightwave technology, this is simple to do.

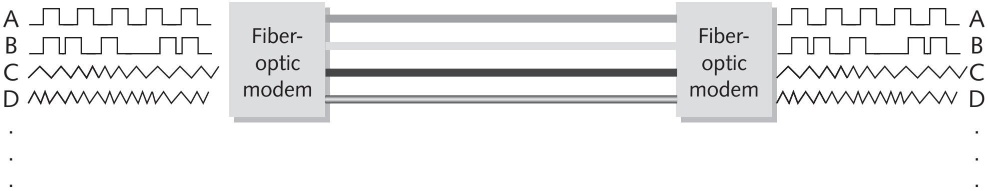

Figure 4-9 Wavelength division multiplexing

Time division multiplexing, statistical multiplexing, and wavelength division multiplexing are most often used in high-bandwidth or long-distance networks such as WANs. You will learn more about transmission technologies that use multiplexing in Chapter 7.

Relationships Between Nodes

So far you have learned about two important characteristics of data transmission: the type of signaling (analog or digital) and the direction in which the signal travels (simplex, half-duplex, duplex, or multiplex). Another important characteristic is the number of senders and receivers, as well as the relationship between them. In general, data communications may involve a single transmitter with one or more receivers, or multiple transmitters with one or more receivers. The remainder of this section introduces the most common relationships between transmitters and receivers.

When a data transmission involves one transmitter and one receiver, it is considered a **point-to-point** transmission. An office building in Dallas exchanging data with another office in St. Louis over a WAN connection is an example of point-to-point transmission. In this case, the sender only transmits data that is intended to be used by a specific receiver. By contrast, **broadcast** transmission involves one transmitter and multiple receivers. For example, a TV station indiscriminately transmitting a signal from its tower to thousands of homes with TVs uses broadcast transmission. A broadcast transmission sends data to any and all receivers, without regard for which receiver can use it. Broadcast transmissions are frequently used on networks because they are simple and quick. They are used to identify certain nodes, to send data to certain nodes (even though every node is capable of picking up the transmitted data, only the destination node will actually do it), and to send announcements to all nodes. Another example of network broadcast transmission is sending video signals to multiple viewers on a network. When used over the Web, this type of broadcast transmission is called **Webcasting**. Figure 4-10 contrasts point-to-point and broadcast transmissions.

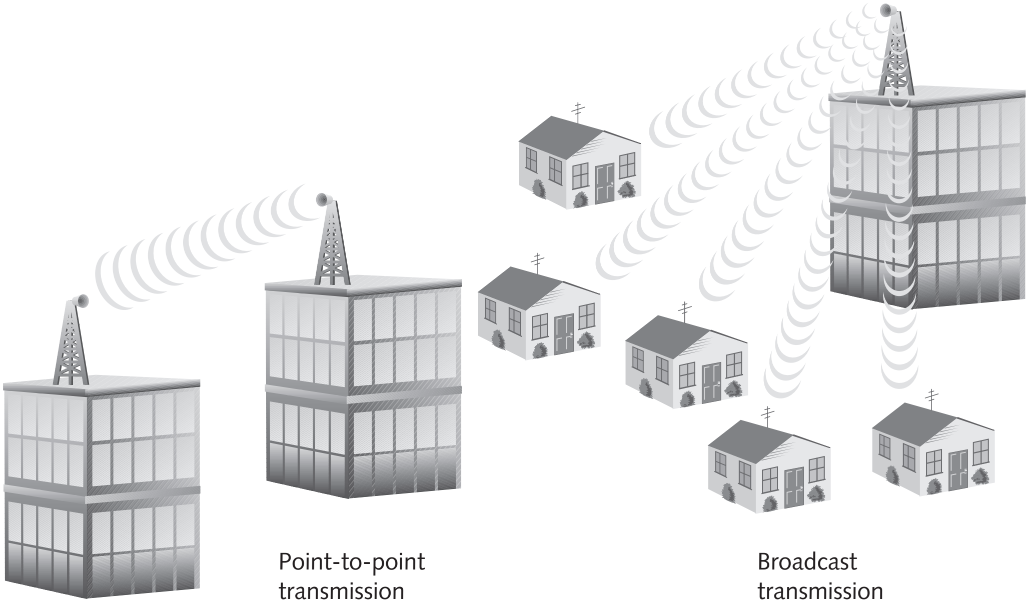

Figure 4-10 Point-to-point versus broadcast transmission

Throughput and Bandwidth

The data transmission characteristic most frequently discussed and analyzed by networking professionals is throughput. **Throughput** is the measure of how much data is transmitted during a given period of time. It may also be called **capacity** or bandwidth (though as you will learn, bandwidth is technically different from throughput). Throughput is commonly expressed as a quantity of bits transmitted per second, with prefixes used to designate different throughput amounts. For example, the prefix "kilo" combined with the word "bit" (as in "kilobit") indicates a 1000 bits per second. Rather than talking about a transmission speed of 1000 bits per second, you would typically say the speed was 1 kilobit per second. Table 4-1 summarizes the terminology and abbreviations used when discussing different throughput amounts. As an example, a typical modem connecting a home PC to the Internet would probably be rated for a maximum throughput of 56.6 Kbps. A very fast LAN might transport up to 1 Gbps of data. The most common contemporary networks achieve throughputs between 10 and 100 Mbps.

Table 4-1 Throughput measures

Quantity	Prefix	Complete Example	Abbreviation
1 bit per second	n/a	1 bit per second	bps
1000 bits per second	kilo	1 kilobit per second	Kbps
1,000,000 bits per second	mega	1 megabit per second	Mbps
1,000,000,000 bits per second	giga	1 gigabit per second	Gbps
1,000,000,000,000 bits per second	tera	1 terabit per second	Tbps

Note

Be careful not to confuse bits and bytes when discussing throughput. Although data storage quantities are typically expressed in multiples of bytes, data transmission quantities (in other words, throughput) are more commonly expressed in multiples of bits per second. Recall that one byte equals 8 bits. When representing different data quantities, a small "b" represents bits, while a capital "B" represents bytes. To put this into context, a modem may transmit data at 56.6 Kbps (kilobits per second); a data file may be 56 KB (kilobytes) in size.

Often, the term "bandwidth" is used interchangeably with throughput, and in fact, this may be the case on the Network+ certification exam. Bandwidth and throughput are similar concepts, but strictly speaking, **bandwidth** is a measure of the difference between the highest and lowest frequencies that a medium can transmit. This range of frequencies, which is expressed in Hz, is directly related to throughput. For example, if the FCC told you that you could transmit a radio signal between 870 and 880 MHz, your allotted bandwidth would be 10 MHz. Because higher frequencies can transmit more data in a given period of time than lower frequencies, bandwidth and throughput are directly related. The higher the bandwidth, the higher the throughput. Later in this chapter, you will discover the throughput characteristics of the most common networking media.

Baseband and Broadband

Baseband is a transmission form in which (typically) digital signals are sent through direct current (DC) pulses applied to the wire. This direct current requires exclusive use of the wire's capacity. As a result, baseband systems can transmit only one signal, or one channel, at a time. Every device on a baseband system shares the same channel. When one node is transmitting data on a baseband system, all other nodes on the network must wait for that transmission to end before they can send data. Baseband transmission supports bidirectional signal flow, which means that computers can both send and receive information on the same length of wire.

Ethernet is an example of a baseband system found on many LANs. In Ethernet (which is described in detail in Chapter 5), each device on a network can transmit over the wire—but only one device at a time. For example, if you want to save a file to the server, your NIC submits your request to use the wire; if no other device is using the wire to transmit data at that time, your workstation can go ahead. If the wire is in use, you must wait and try again later. Of course, this retrying process happens so quickly that you, as the user, may not even notice the wait.

Broadband is a form of transmission in which signals are modulated as radiofrequency (RF) analog pulses that use different frequency ranges. Unlike baseband, broadband technology does not involve digital pulses. Nevertheless, the use of multiple frequencies enables a broadband system to access several channels and, therefore, carry much more data than a baseband system.

As you may know, broadband transmission is used to bring cable TV to your home. Your cable TV connection can carry at least 25 times as much data as a typical baseband system (like Ethernet) carries, including many different broadcast frequencies (channels). In traditional broadband systems, signals travel in only one direction. Therefore, broadband cabling must provide a separate wire for the transmission and the receipt of data. (Because most TV cable provides only one wire, it cannot be used for transmitting data out of your home without some modification. In Chapter 7, you will learn more about using cable to provide Internet access.) Broadband transmission is generally more expensive than baseband transmission because of the extra hardware involved. On the other hand, broadband systems can span longer distances than baseband.

Note

In the field of networking, some terms have more than one meaning, depending on their context. "Broadband" is one of those terms. The "broadband" described in this chapter is the transmission system that carries RF signals across multiple channels on a coaxial cable, as used by cable TV. This definition was the original meaning of broadband. In the discussion of WANs in Chapter 7, the term "broadband" refers to networks that use digital signaling and have very high transmission rates, such as Asynchronous Transfer Mode (ATM) networks.

Transmission Flaws

Both analog and digital signals are susceptible to degradation between the time they are issued by a transmitter and the time they are received. One of the most common transmission flaws affecting data signals is noise. As you learned earlier in this chapter, noise is interference from external sources that may degrade or distort a signal. Many different types of noise may affect transmission. Most of these are caused by one of two electromagnetic phenomenon: **electromagnetic interference (EMI)** or **radiofrequency interference (RFI)**. Both EMI and RFI are waves that emanate from electrical devices or cables carrying electricity. Motors, power lines, televisions, copiers, fluorescent lights, and other sources of electrical activity (including a severe thunderstorm) can cause both EMI and RFI. RFI may also be caused by strong broadcast signals from radio or TV towers. The extent to which noise affects a signal is influenced by the transmission media used to carry the signal. Wireless transmission is typically more susceptible to noise than wireline transmission.

You may be familiar with noise if you have talked on a phone and heard a hissing sound in the background or if you've tried to tune into a distant radio station while driving under strong power lines. When noise affects analog signals, this distortion can result in the incorrect transmission of data, just as if static on the phone line prevented you from hearing the person on the other end of the line. Figure 4-11 shows an analog signal affected by noise.

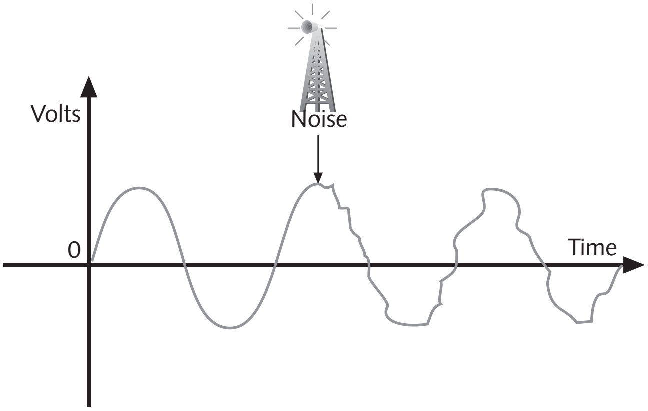

Figure 4-11 An analog signal distorted by noise

While noise affects digital signals, it affects them less severely than analog signals. As shown in Figure 4-12, a digital signal distorted by noise can still be interpreted as a pattern of 1s and 0s.

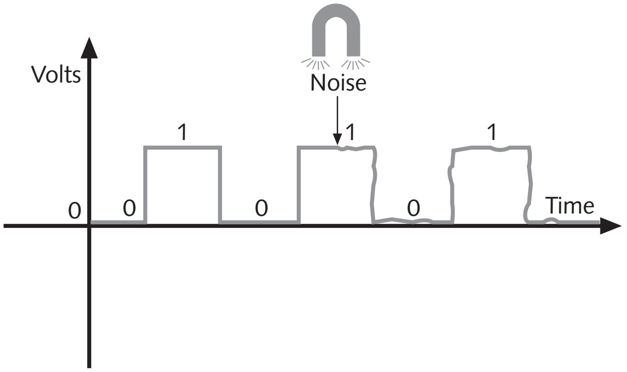

Figure 4-12 A digital signal distorted by noise

Another transmission flaw is **attenuation**, or the loss of a signal's strength as it travels away from its source. In order to compensate for attenuation, both analog and digital signals are strengthened en route to travel farther. However, the technology used to strengthen an analog signal is different from that used to strengthen a digital signal. Analog signals pass through an **amplifier**, an electronic device that increases the voltage, or power, of the signals. When an analog signal is amplified, the noise that it has accumulated is also amplified. This indiscriminate amplification causes the analog signal to progressively worsen. After multiple amplifications, an analog signal may become difficult to decipher. Figure 4-13 shows an analog signal distorted by noise and then amplified once.

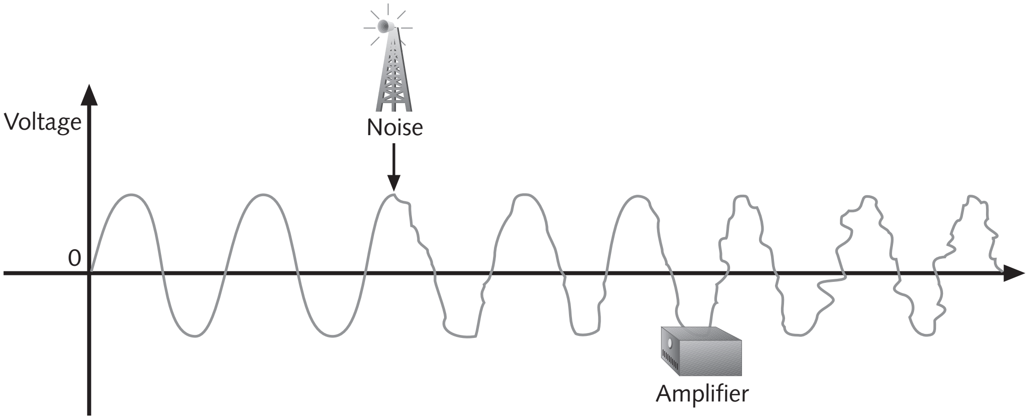

Figure 4-13 An analog signal distorted by noise, and then amplified

When digital signals are repeated, they are actually retransmitted in their original, pure form, without any noise. This process is known as **regeneration**. A device that regenerates a digital signal is called a **repeater**. Figure 4-14 shows a digital signal distorted by noise and then regenerated by a repeater.

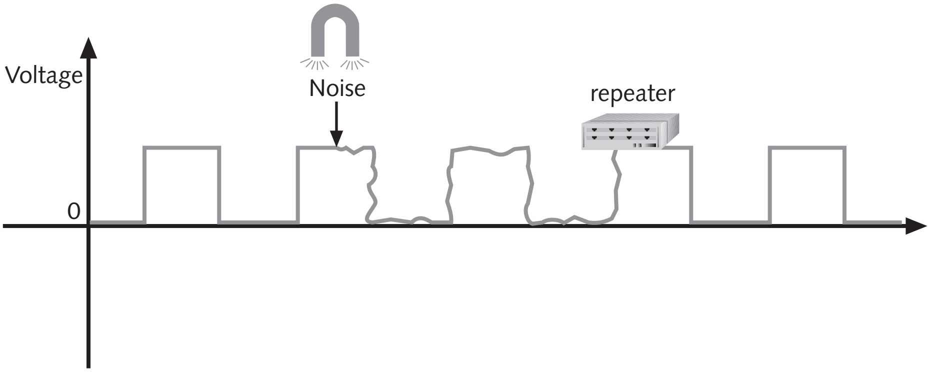

Figure 4-14 A digital signal distorted by noise, and then repeated

Amplifiers and repeaters belong to the Physical layer of the OSI Model. Both are used to extend the length of a network. Since most networks are digital, however, data signals are almost always boosted by repeaters. You will learn more about repeaters in Chapter 6.

Media Characteristics

Now that you are familiar with variations in data signaling, you are ready to understand the transmission media, or the physical or atmospheric paths that these signals traverse. When deciding which kind of transmission media to use, you must match your networking needs with the characteristics of the media. This section describes the characteristics of all types of media. Later, you will learn about the various types of media, and how to choose the appropriate media for your network.

Generally speaking, you must consider five characteristics when choosing a data transfer media: throughput, cost, size and scalability, connectors, and noise immunity. Of course, every networking situation varies; what is significant for one organization may not matter to another. You need to decide what matters most to your organization.

Throughput

Perhaps the most significant factor in choosing a transmission medium is throughput. The physical nature of every transmission medium determines its potential throughput. For example, the laws of physics limit how fast electricity can travel over copper wire, just as they limit how much water can travel through a 1-inch-diameter hose. If you try to direct more water through the 1-inch-diameter hose than it can handle, you will wind up with water splashing back at you or a ruptured hose. Similarly, if you try to push more data through a copper wire than it can handle, the result will be lost data and data errors. Noise and devices connected to the transmission medium can further limit throughput. A noisy circuit spends more time compensating for the noise and, therefore, has fewer resources available for transmitting data.

Cost

The cost implications of transmission media are difficult to pinpoint. While a vendor might quote you the cost per foot of a new type of network cabling, you might have to upgrade some expensive hardware on your network in order to use that type of cabling. Thus, the cost of that cabling would really include more than just the cost of the cabling itself. Not only do media costs depend on the hardware that already exists in a network, but they also depend on the length of your network and the cost of labor in your area (unless you plan to install the cable yourself). The following variables can all influence the final cost of implementing a certain type of media:

- *Cost of installation*—Can you install the media yourself, or must you hire contractors to do it? Will you need to move walls or build new conduits or closets? Will you need to lease lines from a service provider?
- *Cost of new infrastructure versus reusing existing infrastructure*—Can you use existing wiring? In some cases, for example, installing all new Category 7 UTP wiring may not pay off if you can use existing Category 5 UTP wiring. If you replace only part of your infrastructure, will it be easily integrated with the existing media?
- *Cost of maintenance and support*—Reuse of an existing cabling infrastructure does not save any money if it is in constant need of repair or enhancement. Also, if you use an unfamiliar media type, it may cost more to hire a technician to service it. Will you be able to service the media yourself, or must you hire contractors to service it?
- *Cost of a lower transmission rate affecting productivity*—If you save money by reusing existing slower lines, are you incurring costs by reducing productivity? In other words, are you making staff wait longer to save and print reports or exchange e-mail?
- *Cost of obsolescence*—Are you choosing media that may become passing fads, requiring rapid replacement? Will you be able to find reasonably priced connectivity hardware that will be compatible with your chosen media for years to come?

Size and Scalability

Three specifications determine the size and scalability of networking media: maximum nodes per segment, maximum segment length, and maximum network length. In cabling, each of these specifications is based on a physical characteristic of the wire. The maximum number of nodes per segment depends on the attenuation. Each device added to a network segment increases the signal's attenuation slightly. To ensure a clear, strong signal, you must limit the number of nodes on a segment.

The length of a network segment is also limited because of attenuation. After a certain distance, a signal loses so much strength that it cannot be accurately interpreted. Before this deterioration occurs, a repeater on the network must retransmit and amplify the signal. The maximum distance that a signal can travel and still be accurately interpreted equals the maximum segment length. Beyond this length, data loss is apt to occur. As with the maximum number of nodes per segment, maximum segment length varies between different cabling types.

In an ideal world, networks could transmit data instantaneously between sender and receiver, no matter how far apart the two were. Unfortunately, we don't live in an ideal world, and every network is subjected to a delay between the transmission of a signal and its eventual receipt. For example, when you press a key on your computer to save a file to the network, the file's data must travel through your NIC, the network wire, a hub or possibly a switch or router, more cabling, and the server's NIC before it lands on the server's hard disk. Although electrons travel rapidly, they still have to travel, and a brief delay takes place between the moment you press the key and the moment the server accepts the data. This delay is called **latency**.

The length of the cable involved affects latency, as does the existence of any intervening connectivity device, such as a router. The effects of latency become a problem only when a receiving node is expecting some type of communication, such as the rest of a data stream it has begun to accept. If that node does not receive the rest of the data stream, it assumes that no more data is coming. This assumption causes transmission errors on a network. When you connect multiple network segments, you increase the latency in the network. To constrain the latency and avoid its associated errors, each type of cabling is rated for a maximum number of connected network segments.

Connectors

Connectors are the pieces of hardware that connect the wire to the network device, be it a file server, workstation, switch, or printer. Every networking medium requires a specific kind of connector. The type of connectors you use will affect the cost of installing and maintaining the network, the ease of adding new segments or nodes to the network, and the technical expertise required to maintain the network. For example, connectors used with UTP wiring (which look like large telephone wire connectors) are much simpler to insert and replace than are the connectors used with coaxial cabling. UTP wiring connectors are also less expensive and can be used for a variety of cabling designs. You will learn more about the connectors required by different media in this chapter.

Noise Immunity

As you learned earlier, noise (such as EMI from fluorescent lights or motors) can distort data signals. The extent to which noise affects a signal depends partly on the transmission media. Some types of media are more susceptible to noise than others. For example, if you were to issue data signals on a bare copper wire, those signals would be more susceptible to degradation by external EMI sources than signals traveling over a copper wire surrounded by insulation. The type of media least susceptible to noise is fiber-optic cable, because it does not use electric current, but light waves, to conduct signals. In this chapter you will learn how each medium compares in its resistance to noise.

On most networks, noise is an ever-present threat, so you should take measures to limit its impact on your network. For example, you should install cabling well away from powerful electromagnetic forces. If your environment still leaves your network vulnerable, you should choose a type of transmission media that guards the signal-carrying wire from noise. As a general rule, thicker cables are less susceptible to noise, as are cables coated with a protective shielding. It is also possible to use antinoise algorithms to protect data from being corrupted by noise. If these measures don't ward off interference, you may need to use a metal **conduit**, or pipeline, to contain and further protect the cabling.

Now that you understand data transmission and the factors to consider when choosing a transmission medium, you are ready to learn about different types of networking cabling. To qualify for Net+ certification, you must know the characteristics and limitations of each type of cabling, how to install and design a network with each type, and how to provide for future network growth with each cabling option.

Note

The terms "wire" and "cable" are used synonymously in some situations. Strictly speaking, however, "wire" is a subset of "cabling," because the "cabling" category may also include fiber-optic cable, which is almost never called "wire." The exact meaning of the term "wire" depends on context. For example, if you said, in a somewhat casual way, "We had 6 gigs of data go over the wire last night," you would be referring to whatever transmission media helped carry the data—whether fiber, radio waves, coax, or UTP.

Coaxial Cable

Coaxial cable, called "coax" for short, was the foundation for Ethernet networks in the 1980s and remained a popular transmission medium for many years. Over time, however, twisted-pair cabling has replaced coax in most modern LANs. Coaxial cable consists of a central copper core surrounded by an insulator, a braided metal shielding, called

braiding, and an outer cover, called the **sheath** or jacket. Figure 4-15 depicts a typical coaxial cable. The copper core carries the electromagnetic signal, and the braided metal shielding acts as both a shield against noise and a ground for the signal. The insulator layer usually consists of a plastic material such as polyvinyl chloride (PVC) or Teflon. It protects the copper core from the metal shielding, because if the two made contact, the wire would short-circuit. The jacket, which protects the cable from physical damage, may be PVC or a more expensive, fire-resistant plastic.

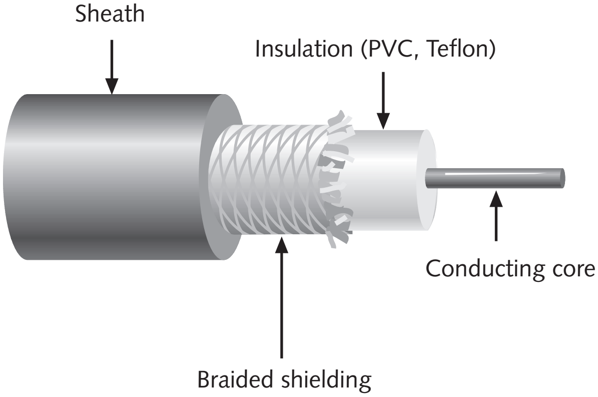

Figure 4-15 Coaxial cable

Because of its insulation and protective braiding, coaxial cable has a high resistance to interference from noise. It can also carry signals farther than twisted-pair cabling before amplification of the signals becomes necessary, although not as far as fiber-optic cabling. On the other hand, coaxial cable is more expensive than twisted-pair cable because it requires significantly more raw materials (such as copper for the core, Teflon for the insulation, and so on) to manufacture. Coaxial cable is also less desirable than twisted-pair because it supports lower throughput.

Coaxial cabling comes in many specifications, although you are likely to see only two or three types of coax in use today. In any case, all types have been assigned an RG specification number. (RG stands for "radio guide," which is appropriate because coaxial cabling is used to guide radiofrequencies in broadband transmission.) The significant differences between the cable types lie in the materials used for their center cores, which in turn influence their impedance (or the resistance that contributes to controlling the signal, as expressed in ohms), throughput, and typical usage. Table 4-2 lists the specifications for several types of coaxial cable. The two with which you should be familiar are RG-58A/U (Thinnet) and RG-8 (Thicknet). As you can see, additional types of coaxial cabling exist (in fact, hundreds more than are represented here), but these are not typically used for data networking.

Table 4-2 Some types of coaxial cable

Designation	Type	Impedance (in ohms)	Description
RG-8	Thickwire	50	Solid core; used for Thicknet LANs
RG-58/U	Thinwire	53.5	Solid copper core; similar to RG-58A/U, but due to insufficient shielding should not be used on Thinnet LANs
RG-58A/U	Thinwire	50	Stranded copper core; used for standard Thinnet LANs
RG-58C/U	Thinwire	50	Military version of RG-58A/U used on Thinnet LANs
RG-59/U	CATV	75	Used for cable TV connections
RG-62A/U	Thickwire	93	Used for IBM 3270 terminals and ARCNet (a nearly obsolete type of network)

Note

RG-59 is the coaxial cabling specification used for cable TV transmission. Because of its different impedance requirements, you cannot use this type of cabling for data networks, even though it might fit your connectors.

Thicknet (10Base5)

Thicknet cabling, also called **thickwire Ethernet**, is a rigid coaxial cable approximately 1-cm thick used for the original Ethernet networks. Because it is often covered with a yellow sheath, Thicknet is sometimes called "yellow Ethernet" or "yellow garden hose." IEEE designates Thicknet as **10Base5** Ethernet. The "10" represents its throughput of 10 Mbps, the "Base" stands for baseband transmission, and the "5" represents the maximum segment length of a Thicknet cable, which is 500 m. You will almost never find Thicknet on new networks, but you may find it on older networks, where it is used to connect one data closet to another as part of the network backbone. A **backbone** is essentially a network of networks; you can think of it as the main route through which data on a network travels. The following is a summary of Thicknet's characteristics:

- *Throughput*—According to the IEEE 802.3 standard, Thicknet transmits data at a maximum rate of 10 Mbps. It can only be used for baseband transmission.
- *Cost*—Thicknet is less expensive than fiber-optic cable, but more expensive than other types of coaxial cabling, such as Thinnet.
- *Connector*—Thicknet networks can include a few different types of connectors, which are very different from those used on modern networks. A **vampire tap**, a connector that pierces a hole in the wire, thus completing a

connection between the metal tooth in the vampire tap and the copper core of the coaxial cable, joins the network cable with a transceiver. The word **transceiver** derives from its function as both a *trans*mitter and re*ceiver* of signals. Since a transceiver is concerned with applying signals to the wire, it belongs in the Physical layer of the OSI Model. Many different types of transceivers exist in networking. On modern (twisted-pair) networks, transceivers are typically built into the NIC. But in the case of Thicknet networking, the transceiver is a separate device and may also be called a **media access unit (MAU)**. A **drop cable**, which connects a networked node to the transceiver, is pictured in Figure 4-16.

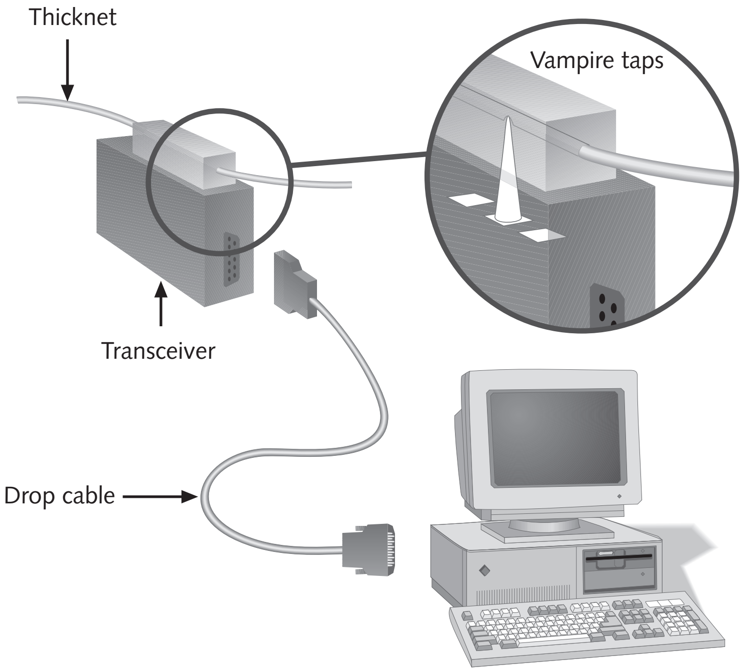

Figure 4-16 Thicknet cable transceiver with detail of a vampire tap

In a Thicknet network, a node's Ethernet interface, a port on the device's NIC, is connected with the drop cable via an AUI connector or an n-series connector. **AUI (Attachment Unit Interface)** is an Ethernet standard that establishes physical specifications for connecting coaxial cables with transceivers and networked nodes. The AUI standard calls for male connectors with 15 pins to connect to the MAU, and female connectors with openings for 15 pins to connect to the network node's Ethernet interface, as shown in Figure 4-17. An AUI connector may also be called a DIX or DB-15 connector. **DIX** stands for Digital, Intel, and Xerox, the three companies that together pioneered Thicknet technology. **DB-15** is a more general term for connectors that use 15 metal pins to complete a connection between devices. "DB" stands for "data bus," while the number "15" indicates how many pins are used to make the connection.

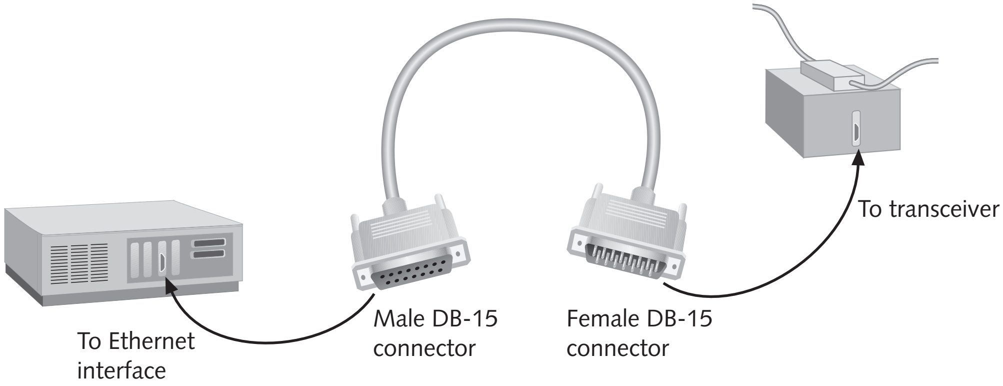

Figure 4-17 AUI connectors

The second type of connector that may be used between a transceiver and a network node (though less frequently) is an **n-series connector** (or **n connector**), as shown in Figure 4-18. In this type of connector, a screw-and-barrel arrangement securely connects coaxial cable segments and devices.

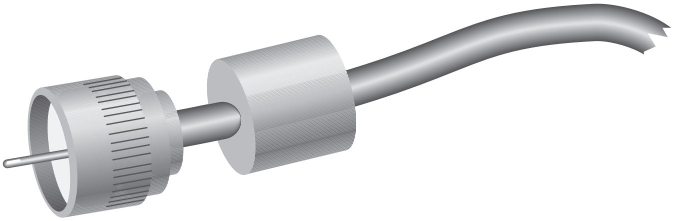

Figure 4-18 N-series connector

- *Noise immunity*—Because of its wide diameter and excellent shielding, Thicknet has the highest resistance to noise of any of the commonly used types of network wiring.

- *Size and scalability*—Because Thicknet has high resistance to noise, it allows data to travel for longer distances than other types of cabling. Its maximum segment length is 500 m, or approximately 1640 feet. Thicknet standards allow for no more than 100 MAUs per segment, and therefore allow a maximum of 100 nodes per segment. Its maximum network length is 1500 m. To minimize the possibility of interference between stations, network devices should be separated by at least 2.5 m.

Thicknet is rarely used on modern networks because of its significant disadvantages. First, this type of cable is difficult to manage. Its rigidity makes it hard to handle and install. Second, it does not allow for network advances because high-speed data transmission cannot run on Thicknet. Although it is less expensive and more resistant to noise than many of the currently popular transmission media, Thicknet is essentially an obsolete technology.

Thinnet (10Base2)

Thinnet, also known as **thin Ethernet**, was the most popular medium for Ethernet LANs in the 1980s. Like Thicknet, Thinnet is rarely used on modern networks, although you may encounter it on networks installed in the 1980s or on newer small office or home office LANs. IEEE has designated Thinnet as 10Base2 Ethernet, with the "10" representing its data transmission rate of 10 Mbps, the "Base" representing the fact that it uses baseband transmission, and the "2" representing its maximum segment length of 185 (or roughly 200) m. Because of its black sheath, Thinnet may also be called "black Ethernet." Thinnet's cable diameter is approximately 0.64 cm, which makes it more flexible and easier to handle and install than Thicknet. More of Thinnet's characteristics are covered in the following list:

- *Throughput*—Thinnet can transmit data at a maximum rate of 10 Mbps, via baseband transmission.
- *Cost*—Thinnet is less expensive than Thicknet and fiber-optic cable, but more expensive than twisted-pair wiring. Prefabricated cables are available for approximately $1/foot. For this reason, Thinnet is sometimes called "cheapnet."
- *Connector*—Thinnet connects the wire to network devices with **BNC T-connectors**, as shown in Figure 4-19. A BNC T-connector with three open ends attaches to the Ethernet interface card at the base of the "T" and to the Thinnet cable at its two sides so as to allow the signal in and out of the NIC. The origin of the acronym "BNC" is somewhat muddy, but probably stands for British Naval Connector. **BNC barrel connectors** (with only two open ends) are used to join two Thinnet cable segments together, as shown in Figure 4-19.

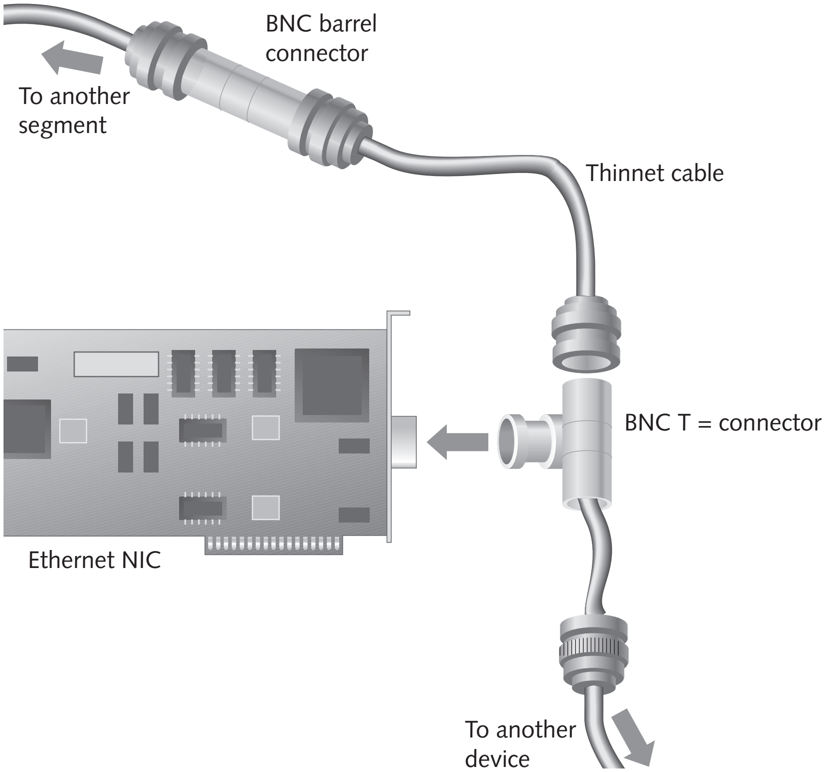

Figure 4-19 Thinnet BNC connectors

- *Size and scalability*— Thinnet allows a maximum of 185 m per network segment, as shown in Figure 4-20. This length is less than that available with Thicknet, because Thinnet's resistance to noise is not as strong. For the same reason, Thinnet can accommodate a maximum of only 30 nodes per segment. Its total maximum network length is slightly more than 550 m. To minimize interference, devices on a Thinnet network should be separated by at least 0.5 m.
- *Noise immunity*—Because of its insulation and shielding, Thinnet is more resistant to noise than twisted-pair wiring. It is not as resistant as Thicknet, however.

Thinnet is occasionally used on modern networks, but more often you will see it on networks installed in the 1980s. Its major advantages are its very low cost and relative ease of use. Because twisted-pair wiring can carry more data and has come down in price, Thinnet has become almost obsolete.

Both Thicknet and Thinnet coaxial cable rely on the bus topology (described in detail in Chapter 5). Recall from Chapter 1 that a topology describes the layout of nodes on a network. In a bus topology, nodes share one, uninterrupted channel. Networks using the bus topology must be terminated at both ends. Without terminators, signals on a bus network would travel endlessly between the two ends of the network, a phenomenon known as **signal bounce**. Figure 4-20 depicts a 10Base2 network using a bus topology.

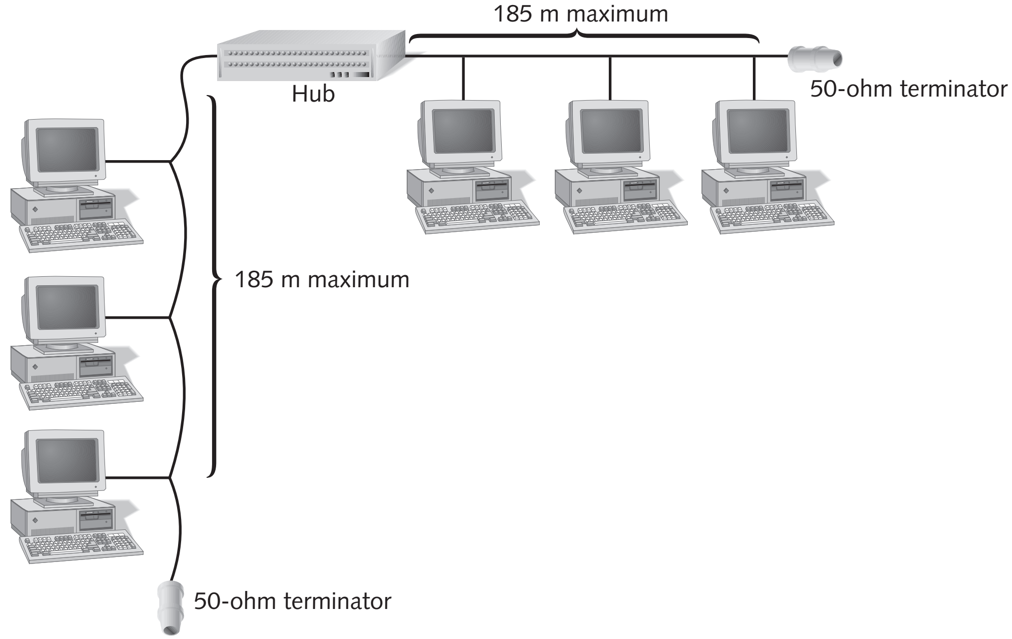

Figure 4-20 A 10Base2 Ethernet network

Thicknet and Thinnet cable both require 50-ohm resistors terminating either end of the network. These cables must also be grounded at one end. If you ground a coaxial network at both ends, or if you don't ground it at all, the network will generate intermittent data transmission errors.

TWISTED-PAIR CABLE

Twisted-pair (TP) cable is similar to telephone wiring and consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm, or 22-24 AWG (American Wire Gauge) standard copper wires. The wires are twisted around each other to form pairs and all the pairs are encased in a plastic sheath, as shown in Figure 4-21. The twists in the wire help to reduce the effects of crosstalk. **Crosstalk**, which is measured in decibels (dB), occurs when signals traveling on nearby wire pairs infringe on another pair's signal. If you envision the wire pairs in a single cable as couples in an elevator, you can imagine how one couple speaking very loudly might impair the other couple's ability to converse. Because they are twisted around each other, the release of current from one wire cancels out the release of current from the adjacent wire. Another form of crosstalk, called

alien crosstalk, can occur when signals from an adjacent cable (as opposed to adjacent wires) interfere with another cable's transmission. Alien crosstalk becomes a real threat when network administrators bundle more cables into smaller conduits.

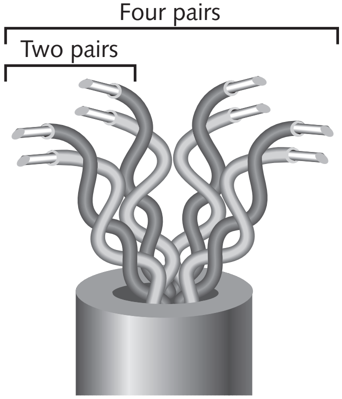

Figure 4-21 Twisted-pair cable

The more twists per inch in a pair of wires, the more resistant the pair will be to all forms of noise. Higher-quality, more expensive twisted-pair cable contains more twists per foot. The number of twists per meter or foot is known as the **twist ratio**. Because twisting the wire pairs more tightly requires more cable, however, a high twist ratio can result in greater attenuation. For optimal performance, cable manufacturers must strike a balance between crosstalk and attenuation reduction.

Because twisted-pair is used in such a wide variety of environments and for a variety of purposes, it comes in hundreds of different designs. These designs vary in their twist ratio, the number of wire pairs that they contain, the grade of copper used, the type of shielding (if any), and the materials used for shielding, among other things. A twisted-pair cable may contain from 1 to 4200 wire pairs. Early network cables incorporated two wire pairs: one pair dedicated to sending data and one pair dedicated to receiving data. Modern networks typically use cables containing four wire pairs, with more than one wire pair both sending and transmitting data simultaneously.

In 1991, two standards organizations, TIA (Telecommunications Industry Association) and EIA (Electronic Industries Alliance), finalized their specifications for twisted-pair wiring in a standard called TIA/EIA 568. Since then, TIA has become part of EIA, and this new body has continually revised the international standards for new and modified transmission media. Its standards now cover cabling media, design, and installation specifications. The TIA/EIA 568 standard divides twisted-pair wiring into several categories. Thus you will hear twisted-pair referred to as CAT (category) 1, 2, 3, 4, 5, 6, and now, CAT7. All of these cables fall under the TIA/EIA 568 standard. Modern LANs most frequently use CAT5 or higher wiring.

Twisted-pair cable is the most common form of cabling found on LANs today. It is relatively inexpensive, flexible, and easy to install, and it can span a significant distance before requiring a repeater (though not as far as coax). Twisted-pair cable easily accommodates several different topologies, although it is most often implemented in star or star-hybrid topologies. Furthermore, twisted-pair can handle the faster networking transmission rates currently being employed. Due to its wide acceptance, it will probably be updated to handle the even faster rates that will emerge in the future. One drawback to twisted-pair is that, because of its flexibility, it is more prone to physical damage than coaxial cable. This problem is a minor factor given its many advantages over coax. All twisted-pair cable falls into one of two categories: shielded twisted-pair (STP) or unshielded twisted-pair (UTP).

Shielded Twisted-Pair (STP)

As the name implies, **shielded twisted-pair (STP)** cable consists of twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil. Some STP use a braided metal shielding. The shielding acts as a barrier to external electromagnetic forces, thus preventing them from affecting the signals traveling over the wire inside the shielding. The shielding may be grounded to enhance its protective effect. The effectiveness of STP's shield depends on the level and type of environmental noise, the thickness and material used for the shield, the grounding mechanism, and the symmetry and consistency of the shielding. Figure 4-22 depicts an STP cable.

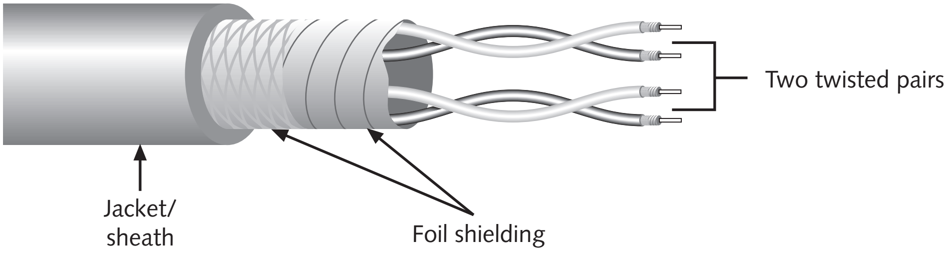

Figure 4-22 STP cable

Unshielded Twisted-Pair (UTP)

Unshielded twisted-pair (UTP) cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP. Figure 4-23 depicts a typical UTP cable.

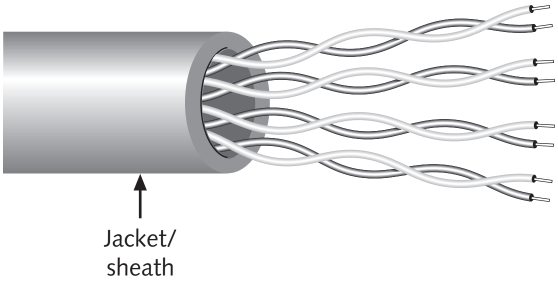

Figure 4-23 UTP cable

Earlier, you learned that the TIA/EIA consortium designated standards for twisted-pair wiring. To manage network cabling, you need to be familiar with the standards that may be used on modern networks, particularly CAT3 and CAT5 or higher.

- *Category 1 (CAT1)*—A form of UTP that contains two wire pairs. CAT1 is suitable for voice communications but not for data. With advanced signaling techniques, it can carry up to 128 kilobits per second (Kbps) of data.
- *Category 2 (CAT2)*—A form of UTP that contains four wire pairs and can carry up to 4 Mbps of data. CAT2 is rarely found on modern networks, however, because most systems require higher throughput.
- *Category 3 (CAT3)*—A form of UTP that contains four wire pairs and can carry up to 10 Mbps of data with a possible bandwidth of 16 MHz. CAT3 has typically been used for 10 Mbps Ethernet or 4 Mbps Token Ring networks. Network administrators are gradually replacing their existing CAT3 cabling with CAT5 to accommodate higher throughput.
- *Category 4 (CAT4)*—A form of UTP that contains four wire pairs and can support up to 16 Mbps throughput. CAT4 may be used for 16 Mbps Token Ring or 10 Mbps Ethernet networks. It is guaranteed for signals as high as 20 MHz and provides more protection against crosstalk and attenuation than CAT1, CAT2, or CAT3.
- *Category 5 (CAT5)*—The most popular form of UTP for new network installations and upgrades to Fast Ethernet. CAT5 contains four wire pairs and supports up to 100 Mbps throughput and a 100 MHz signal rate. In addition to 100 Mbps Ethernet, CAT5 wiring can support other fast networking technologies. Figure 4-24 depicts a typical CAT5 UTP cable with its twisted pairs untwisted, allowing you to see their matched color coding. For example, the wire that is colored solid orange is twisted around the wire that is part orange and part white to form the pair responsible for transmitting data.
- *Enhanced Category 5 (CAT5e)*—A higher-grade version of CAT5 wiring that contains high-quality copper, offers a high twist ratio, and uses advanced

methods for reducing crosstalk. Enhanced CAT5 can support a signaling rate as high as 200 MHz, double the capability of regular CAT5.

- *Category 6 (CAT6)*—A twisted-pair cable that contains four wire pairs, each wrapped in foil insulation. Additional foil insulation covers the bundle of wire pairs, and a fire-resistant plastic sheath covers the second foil layer. The foil insulation provides excellent resistance to crosstalk and enables CAT6 to support at least six times the throughput supported by regular CAT5. Because it is new and because most network technologies cannot exploit its superlative capacity, CAT6 is rarely encountered in today's networks.
- *Category 7 (CAT7)*—A twisted-pair cable that contains multiple wire pairs, each surrounded by its own shielding, then packaged in additional shielding beneath the jacket. While standards have not yet been finalized for CAT7, some cable supply companies are selling it, and organizations are installing it. One advantage to CAT7 cabling is that it can support signal rates up to 1 GHz. However, it requires different connectors than other versions of UTP because its twisted pairs must be more isolated from each other to ward off crosstalk. Because of its added shielding, CAT7 cabling is also larger and less flexible than other versions of UTP cable. For the same reasons that CAT6 is not typically found on modern networks, CAT7 is also rare; but it will likely become popular as the final standard is released and networks are upgraded.

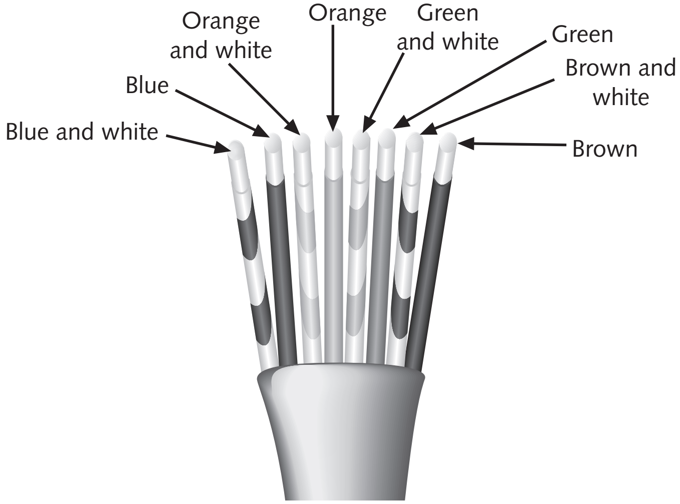

Figure 4-24 A CAT5 UTP cable

UTP cabling may be used with any one of several IEEE Physical layer networking standards. Recall that IEEE standards specify how signals are transmitted to the media. The following sections describe these standards, which you must understand in order to obtain Network+ certification.

10BaseT

10BaseT is a popular Ethernet networking standard that replaced the older 10Base2 and 10Base5 technologies. The "10" represents its maximum throughput of 10Mbps, the "Base" indicates that it uses baseband transmission, and the "T" stands for twisted pair, the medium it uses. On a 10BaseT network, one pair of wires in the UTP cable is used for transmission, while a second pair of wires is used for reception. By using two pairs of wires, 10BaseT networks use full-duplex transmission. A 10BaseT network requires CAT3 or higher UTP.

Nodes on a 10BaseT Ethernet network connect to a central hub or repeater in a star fashion. As is typical of a star topology, a single network cable connects only two devices. This characteristic makes 10BaseT networks more fault-tolerant than 10Base2 or 10Base5, both of which use the bus topology. It also means that 10BaseT networks are easier to troubleshoot because you can isolate problems more readily when every device has a separate connection to the LAN. Figure 4-25 depicts a small 10BaseT Ethernet network.

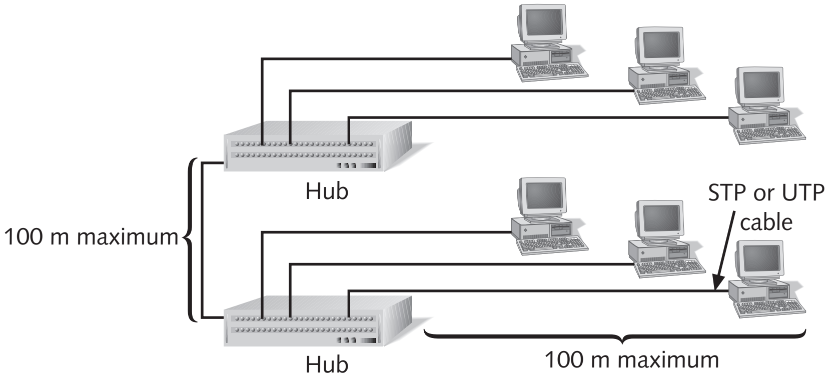

Figure 4-25 A 10BaseT Ethernet network

10BaseT, like 10Base2 and 10Base5, is also subject to a distance limitation. The maximum distance that a 10BaseT segment can traverse is 100 meters. To go beyond that distance, Ethernet star segments must be connected by additional hubs or switches to form more complex topologies (discussed in the next chapter). This arrangement can connect a maximum of five sequential network segments. Figure 4-26 illustrates how 10BaseT segments can be interconnected to form an enterprise-wide network. An **enterprise-wide network** is one that spans an entire organization and often services the needs of many diverse users. It may include many locations (as a WAN), or it may be confined to one location but include many different departments, floors, and network segments.

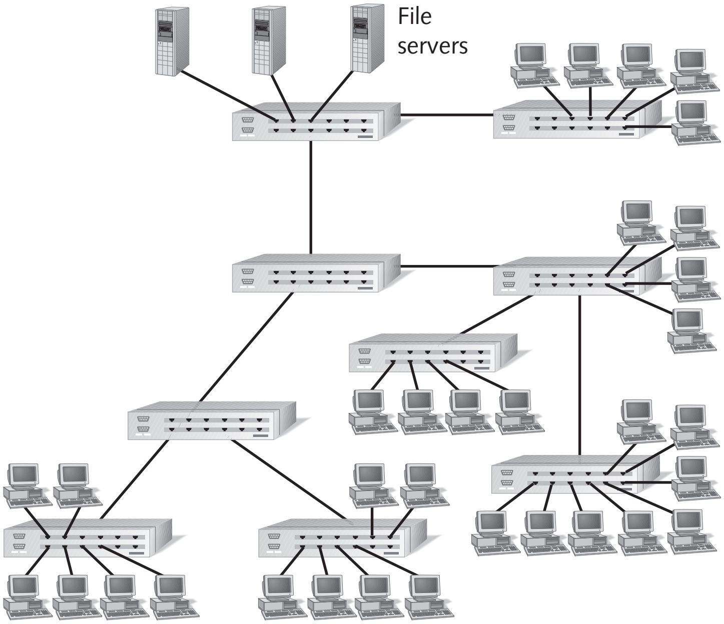

Figure 4-26 Interconnected 10BaseT segments

100BaseT

As networks become larger and handle heavier traffic, Ethernet's longstanding 10 Mbps limitation becomes a bottleneck that detrimentally affects response time. The need for faster LANs that can use the same infrastructure as the popular 10BaseT technology has been met by **100BaseT**, also known as **Fast Ethernet**. 100BaseT, specified in the IEEE 802.3u standard, enables LANs to run at a 100-Mbps data transfer rate, a tenfold increase from that provided by 10BaseT, without requiring a significant investment in new infrastructure. 100BaseT uses baseband transmission and the same, star topology as 10BaseT. It also uses the same RJ-45 data connectors. Depending on the type of 100BaseT technology used, it may require CAT3 or CAT5 or higher UTP.

As with 10BaseT, nodes on a 100BaseT network are configured in a star topology and the length between an end node and the hub for 100BaseT networks cannot exceed 100 meters. Multiple hubs can be connected on buses to extend the network, but 100BaseT buses can practically support a maximum of three network segments connected with two hubs.

Two 100BaseT specifications—100BaseT4 and 100BaseTX—have competed for popularity as organizations move to 100-Mbps technology. The difference between these technologies relates primarily to the way they achieve the 100-Mbps transmission rate, which affects their cabling requirements.

- **100BaseTX**—This is the version you are most likely to encounter. It achieves its speed by sending the signal 10 times faster and condensing the time between digital pulses as well as the time a station must wait and listen for a signal. 100BaseTX requires CAT 5 or higher unshielded twisted-pair cabling. Within the cable, it uses the same two pairs of wire for transmitting and receiving data that 10BaseT uses. Therefore, like 10BaseT, 100BaseTX is also capable of full-duplex transmission. Full duplexing can potentially double the bandwidth of a 100BaseT network to 200 Mbps.

- **100BaseT4**—This version is differentiated from 100BaseTX in that it uses all four pairs of wires in a UTP cable, and, therefore, can use lower-cost CAT 3 wiring. It achieves its speed by breaking the 100-Mbps data stream into three streams of 33-Mbps each. These three streams are sent over three pairs of wire in the cable. However, because 100BaseT4 technology uses all four wire pairs for unidirectional signaling, it cannot support full duplexing. One reason 100BaseT4 is less popular than 100BaseTX is because it cannot support full duplexing.

Caution

You cannot mix 100BaseTX and 100BaseT4 on a single network segment. For example, if you purchase a hub designed for 100BaseTX transmission, you cannot use NICs designed for 100BaseT4 transmission to connect to that hub.

100BaseVG

A cousin of the Ethernet 100 Mbps technologies is **100BaseVG**, also called **100VG-AnyLAN**. The "VG" stands for voice grade. 100BaseVG, which was originally developed by Hewlett-Packard and AT&T, is now governed by IEEE standard 802.12. A significant difference between 100BaseVG and 100BaseT is the way in which they allow network nodes to transmit data on the network. 100BaseVG employs a more efficient and accurate process that allows it to better serve networks that carry audio, video, or other time-sensitive data (explaining the "voice grade" specification). However, this technology also requires more sophisticated NICs and connectivity devices than 100BaseT networks use. You will learn more about this technology in the following chapter.

Another disadvantage of 100BaseVG is that the time the hub takes to process each request reduces the network's overall performance, so that it cannot usually match the speed of a 100BaseT network. Also, 100BaseVG uses all four wire pairs in a UTP cable, and, therefore, cannot take advantage of full duplexing, which can potentially double a network's bandwidth. For these reasons, and because compatible equipment may be hard to find, 100BaseVG is not widely implemented.

Comparing STP and UTP

STP and UTP share several characteristics. The following list highlights their similarities and differences.

- *Throughput*—STP and UTP can both transmit data up to 100 Mbps (and with newer technology, potentially higher), depending on the grade of cabling and the transmission method in use.

- *Cost*—STP and UTP vary in cost, depending on the grade of copper used, the category rating, and any enhancements. Typically, STP is more expensive than UTP because it contains more materials and it has a lower demand. High-grade UTP, however, can be very expensive. For example, CAT6 costs more per foot than regular CAT5 cabling. As new types of cabling are released, they initially cost significantly more than older types of cabling. However, as they remain on the market and become more widely accepted, their price drops.
- *Connector*—STP and UTP use **RJ-45** connectors and data jacks, which look similar to telephone connectors and jacks. "RJ" stands for registered jack. Figure 4-27 shows a close-up of an RJ-45 connector for a cable containing four wire pairs. The section on "Installing Cable" later in this chapter describes the use of RJ-45 connectors and data jacks in more detail.

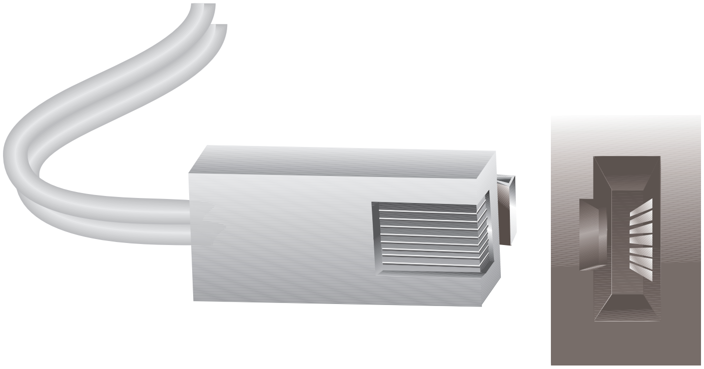

Figure 4-27 An RJ-45 connector

- *Noise immunity*—Because of its shielding, STP is more noise-resistant than UTP is. On the other hand, UTP may use filtering and balancing techniques to offset the effects of noise.
- *Size and scalability*—The maximum segment length for both STP and UTP is 100 m, or 328 feet. This span is less than that available with coaxial cable because twisted-pair is more susceptible to environmental noise. Twisted-pair can accommodate a maximum of only 1024 nodes per logical segment. Its maximum network length depends on the type of signaling used, as discussed in the following section.

Fiber-Optic Cable

Fiber-optic cable, or simply *fiber*, contains one or several glass fibers at its center, or **core**. Data are transmitted via pulsing light sent from a laser or light-emitting diode (LED) through the central fibers. Surrounding the fibers is a layer of glass called **cladding.** The cladding glass is a different density from the glass in the strands. It acts as a mirror, reflecting light back to the core in patterns that vary depending on the transmission mode. This reflection allows the fiber to bend around corners without diminishing the integrity of the light-based signal. Outside the cladding, a plastic buffer protects the glass cladding and core. Since it is opaque, it also absorbs any light that might escape. To prevent the cable from stretching, and to further protect the inner core, strands of Kevlar (an advanced polymeric fiber) surround the plastic buffer. Finally, a plastic sheath covers the strands of Kevlar. Figure 4-28 shows the different layers of a fiber-optic cable.

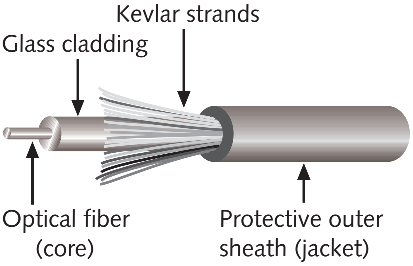

Figure 4-28 A fiber-optic cable

Like twisted-pair cable, fiber comes in a number of different types. Fiber cable variations fall into two categories: single-mode and multimode. **Single-mode fiber** uses a narrow core (less than 10 microns in diameter) through which light generated by a laser travels over one path, reflecting very little. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows single mode fiber to accommodate high bandwidths and long distances (without requiring repeaters). Single-mode fiber may be used to connect a carrier's two facilities. However, it costs too much to be considered for use on typical data networks. **Multimode fiber** contains a core with a larger diameter than single-mode fiber (between 50 and 100 microns in diameter) over which many pulses of light generated by a light emitting diode (LED) travel at different angles. Because light is being reflected many different ways in a multimode fiber cable, the waves become less easily distinguishable the longer they travel. Thus, multimode fiber is best suited for shorter distances than single-mode fiber. It is commonly found on cables that connect a router to a switch or a server on the backbone of a network. Figure 4-29 graphically depicts the differences between single-mode and multimode fiber.

Because of its reliability, fiber is currently used primarily as a cable that connects the many segments of a network. Experts predict, however, that it will replace UTP as the primary means of bringing data to the desktop within the next decade. Fiber-optic cable provides the benefits of nearly unlimited throughput, very high resistance to noise, and excellent security. Because fiber does not conduct electricity like copper wire, it does not emit a current. As a result, the signals it carries stay within the fiber and cannot easily be picked up except at the destination node. Copper, on the other hand, generates a signal that can be monitored by taps into the network. Fiber can also carry signals for longer distances than can coax or twisted-pair cable. In addition, you can use longer lengths of fiber with fewer repeaters than on a copper-based network. Finally, fiber is widely accepted by the high-speed networking industry. Thus, industry groups are establishing standards to ensure that fiber networking equipment from multiple manufacturers can be integrated without difficulty.

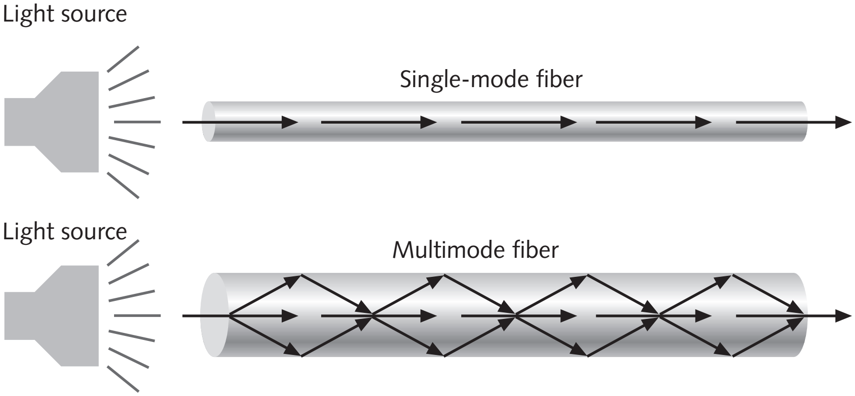

Figure 4-29 Single-mode and multimode fiber-optic cables

The most significant drawback to the use of fiber is its high cost. Another disadvantage is that fiber can transmit data in only one direction at a time; to overcome this drawback, each cable must contain two strands—one to send data and one to receive it. Finally, unlike copper wiring, fiber is difficult to splice, which means quickly repairing a cable in the field (given little time or resources) is difficult if not impossible. Fiber's characteristics are summarized following.

- *Throughput*—Fiber has proved reliable in transmitting data at rates as high as 1 gigabit (or 1000 megabits) per second. With further improvements expected, fiber will probably surpass that limit in the future. Fiber's amazing throughput is partly due to the physics of light traveling over glass. Unlike electrical pulses traveling over copper, the light experiences virtually no resistance and, therefore, can be reliably transmitted at faster rates than electrical pulses. In fact, a pure glass strand can accept up to 1 billion laser light pulses per second. Because of its high cost, however, fiber is currently found almost exclusively on backbone lengths. Nevertheless, its high throughput capability also makes it suitable for applications that generate a great deal of traffic, such as video or audio conferencing.

- *Cost*—Fiber is the most expensive type of cable. The cost of running fiber to every desktop is currently prohibitive; consequently, fiber is typically used only for long-distance transmission or network backbones that must bear extraordinary amounts of traffic. Not only is the cable itself more expensive than metal cabling, but fiber-optic NICs and hubs can cost as much as five times more than NICs and hubs designed for UTP networks. In addition, hiring skilled fiber cable installers costs more than hiring twisted-pair cable installers.

- *Connector*—With fiber cabling, you can use any of 10 different types of connectors. Figure 4-30 shows two popular connector types, an ST connector and an SC connector. For short connections, such as 2-foot cable between a router and a patch panel, you should consider purchasing fiber cables with the connectors pre-installed. For longer connections, either you or the technician who installs your fiber can attach the connectors to the cable.

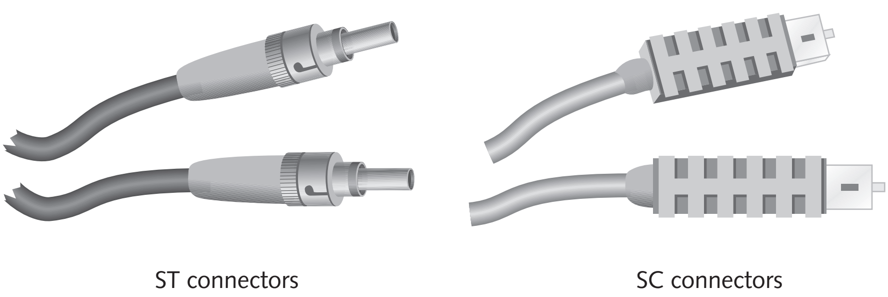

Figure 4-30 ST and SC fiber connectors

- *Noise immunity*—Since fiber does not conduct electrical current to transmit signals, it is unaffected by either EMI or RFI. Its impressive noise resistance is one reason why fiber can span such long distances before it requires repeaters to regenerate its signal.
- *Size and scalability*—Network segments made from fiber can span 100 m. Overall network lengths vary depending on the type of fiber-optic cable used. For multimode fiber, TIA/EIA recommends a segment limit of 2 km. For single-mode fiber, the limit is 3 km. Although signals transmitted over fiber do not suffer interference, they do experience **optical loss**, or the degradation of the light signal. Optical loss accrues over long distances and grows with every connection point in the fiber network. Dust or oil in a connection (for example, from people handling the fiber while splicing it) can further exacerbate optical loss.

Like twisted-pair and coaxial cabling, fiber-optic cabling comes in a number of different varieties, depending on its intended use and the manufacturer. For example, one type of fiber-optic cabling, the D series, is used for underground conduits to high-volume telecommunications carriers (such as AT&T or Global Crossing). This cable may contain as many as 1000 fibers and be heavily sheathed to prevent damage caused by rodents gnawing on it. At the other end of the spectrum, fiber-optic patch cables for use on LANs may contain only two strands of fiber and be pliable enough to bend easily around corners.

Just as with twisted-pair and coaxial cabling, IEEE has established Physical layer standards for networks that use fiber-optic cable. Two of the most important standards are described below.

10BaseF

In the **10BaseF** standard, the "10" represents its maximum throughput of 10 Mbps, "Base" indicates its use of baseband transmission, and "F" indicates that it relies on a medium of fiber-optic cable. In fact there are at least three different kinds of 10BaseF. All require two strands of multimode fiber. One strand is used for data transmission and one strand is used for reception, making 10BaseF a full-duplex technology. All versions of 10BaseF also require ST type of connectors on their patch cables, NICs, and connectivity devices. The maximum segment length for 10BaseF may be 1000 or 2000 meters, depending on the version used. It may contain no more than two repeaters per network. Like 10BaseT, 10BaseF makes use of the star topology, with its repeaters connected through a bus.

Since 10BaseF involves (expensive) fiber and achieves merely 10 Mbps throughput (whereas the fiber medium is capable of much higher throughput), it is not commonly found on modern networks.

100BaseFX

The **100BaseFX** standard specifies a network capable of 100-Mbps throughput that uses baseband transmission and fiber-optic cabling. Like 10BaseF, 100BaseFX requires multimode fiber containing at least two strands of fiber. One strand is used for data transmission, while the other strand is used for reception, making 100BaseFX a full-duplex technology. 100BaseFX networks require one of several types of connectors, including the two most popular connectors, SC and ST. Its maximum segment length is 400 meters, with a maximum of two repeaters allowed to connect segments. The 100BaseFX standard uses a star topology, with its repeaters connected through a bus.

100BaseFX, like 100BaseT, is also considered "Fast Ethernet." Organizations switching, or migrating, from UTP to fiber media can combine 100BaseTX and 100BaseFX within one network. In order to do this, connectivity devices must have both RJ-45 and SC or ST ports. Alternately, a 100BaseTX to 100BaseFX media converter may be used at any point in the network to interconnect the different media and convert the signals of one standard to signals that work with the other standard.

Tip

In Ethernet technology, the most common network speeds are 10 Mbps and 100 Mbps. Actual data transfer rates on a network will vary, just as you might average 25 miles per gallon (mpg) driving your car to work and back, even though the manufacturer rates the car's gas mileage at 30 mpg.

Physical Layer Networking Standards

In order to obtain Network+ certification, you must be familiar with the different characteristics and limitations of each physical networking medium discussed in this chapter. To put this information in context, Table 4-3 summarizes the characteristics and limitations for Physical layer networking standards, including Ethernet networks that use coaxial cable, twisted-pair cable, and fiber-optic cable.

Table 4-3 Physical layer networking standards

Standard	Maximum Transmission Speed (Mbps)	Maximum Distance per Segment (m)	Physical Media	Simple Physical Topology Used
10Base5	10	500	Thick coaxial cable	Bus
10Base2	10	185	Thin coaxial cable	Bus
10BaseT	10	100	Unshielded twisted-pair	Star
100BaseTX	100	100	Unshielded twisted-pair	Star
100BaseT4	100	100	Unshielded twisted-pair	Star
100BaseVG	100	100	Unshielded twisted-pair	Star
10BaseF	10	1000 or 2000, depending on version	Multimode fiber	Star
100BaseFX	100	400	Multimode fiber	Star

Note

Some networks may use more than one type of physical media. For instance, 100BaseTX could run on fiber, even though the minimum standard is unshielded twisted-pair cabling. The latest unshielded twisted-pair may be able to carry data at 1Gbps, albeit with severe distance limitations, so fiber is recommended.

Cable Design and Management

For a long time, organizations took their **cable plant**—the hardware that makes up the enterprise-wide cabling system—for granted. Because of increasing traffic demands and business's increasing reliance on networks, however, organizations must now actively manage their physical infrastructure. Proactive cable design and management make moves and expansion smoother and limit productivity losses due to Physical layer problems. Although it doesn't get as much attention as asset management or security concerns, cable management is a significant element of a sound network management strategy.

In 1991, TIA/EIA released its joint 568 Commercial Building Wiring Standard, also known as **structured cabling**, for uniform, enterprise-wide, multivendor cabling systems. Structured cabling suggests how networking media can best be installed to maximize performance and minimize upkeep. Structured cabling specifies standards without regard for the type of media or transmission technology used on the network. In other words, it is designed to work just as well for 10BaseT networks as it does for 100BaseFX networks. Structured cabling is based on a hierarchical design that divides cabling into six subsystems, described in the following list. You should be familiar with the principles of structured cabling before you attempt to design, install, or troubleshoot an organization's cable plant. Figure 4-31 illustrates how the six subsystems fit together.

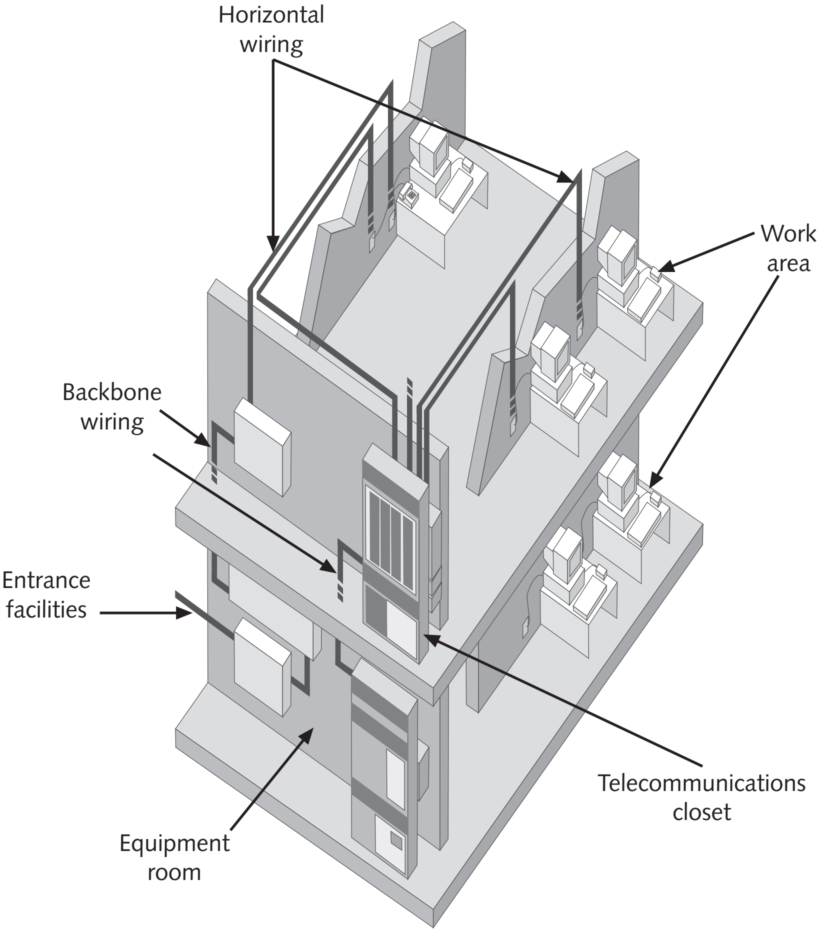

Figure 4-31 TIA/EIA structured cabling subsystems

- *Entrance facilities*—The point at which a building's internal cabling plant begins. The entrance facility separates LANs from WANs and designates where the telecommunications service carrier (whether it's a local phone company, dedicated, or long-distance carrier) accepts responsibility for the (external) wire.

- *Backbone wiring*—As you learned earlier, a backbone is essentially a network of networks. Backbone wiring provides interconnection between telecommunications closets, equipment rooms, and entrance facilities. On a campus-wide network, the backbone includes not only vertical connectors between floors, or **risers**, and cabling between equipment rooms, but also cabling between buildings. You will learn more about backbone topology and design in Chapter 5. The TIA/EIA standard designates distance limitations for backbones of varying cable types, as specified in Table 4-4. On modern networks, backbones are usually composed of fiber-optic or UTP cable. The cross connect is the central connection point for the backbone wiring.

Table 4-4 TIA/EIA specifications for backbone cabling

Cable Type	Cross-Connects to Telecommunications Room	Equipment Room to Telecommunications Room	Cross-Connects to Equipment Room
UTP	800 m (voice specification)	500 m	300 m
Single-mode fiber	3000 m	500 m	1500 m
Multimode fiber	2000 m	500 m	1500 m

- *Equipment room*—The location where significant networking hardware, such as servers and mainframe hosts, resides. Cabling to equipment rooms usually connects telecommunications closets. On a campus-wide network, each building may have its own equipment room.
- *Telecommunications closet*—A "telco room" that contains connectivity for groups of workstations in its area, plus cross connections to equipment rooms. Large organizations may have several telco rooms per floor. Telecommunications closets typically house patch panels, punch-down blocks, hubs or switches, and possibly other connectivity hardware. A **punch-down block** is a panel of data receptors into which horizontal cabling from the workstations is inserted. If used, a **patch panel** is a wall-mounted panel of data receptors into which patch cables from the punch-down block are inserted. Figure 4-32 shows examples of a punch-down block and a patch panel. Finally, patch cables connect the patch panel to the hub or switch. Because telecommunications closets are usually small, enclosed spaces, good cooling and ventilation systems are important to maintaining a constant temperature in telco rooms.

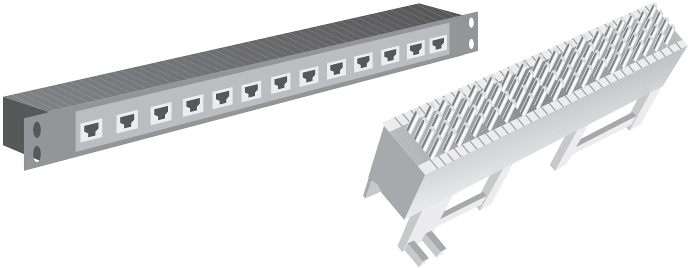

Figure 4-32 Patch panel (left) and punch-down block (right)

- *Horizontal wiring*—Wiring that connects workstations to the closest telecommunications closet. TIA/EIA recognizes three possible cabling types for horizontal wiring: STP, UTP, or fiber-optic. The maximum allowable distance for horizontal wiring is 100 m. This span includes 90 m to connect a data jack on the wall to the telecommunications closet plus a maximum of 10 m to connect a workstation to the data jack on the wall. Figure 4-33 depicts a horizontal wiring configuration.

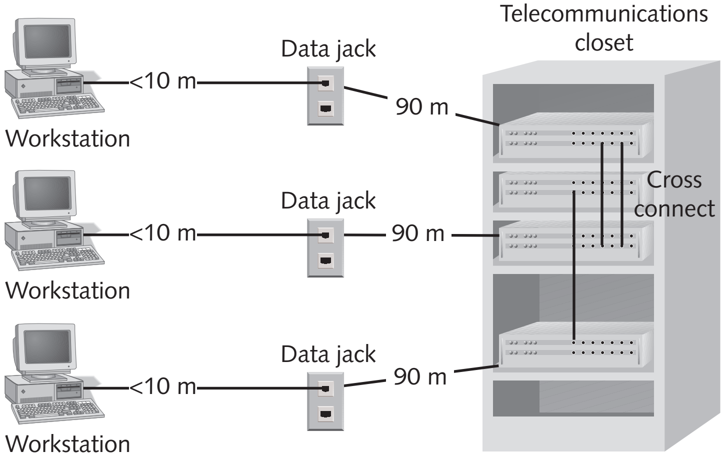

Figure 4-33 Horizontal wiring

- *Work area*—An area that encompasses all patch cables and horizontal wiring necessary to connect workstations, printers, and other network devices from their NICs to the telecommunications closet. A **patch cable** is a relatively short section (usually between 3 and 25 feet long) of twisted-pair cabling with connectors on both ends that connects network devices to data outlets. The TIA/EIA standard calls for each wall jack to contain at least one voice and one data outlet, as pictured in Figure 4-34. Realistically, you will encounter a variety of wall jacks. For example, in a student computer lab lacking phones, a wall jack with a combination of voice and data outlets is unnecessary.

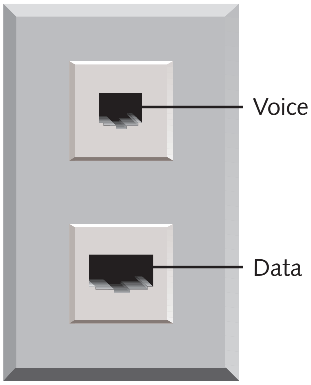

Figure 4-34 A standard TIA/EIA wall jack

Figure 4-35 depicts one possible example of a structured cabling hierarchy. The TIA/EIA standard dictates that a single hierarchy contain no more than two levels of cross-connection wiring.

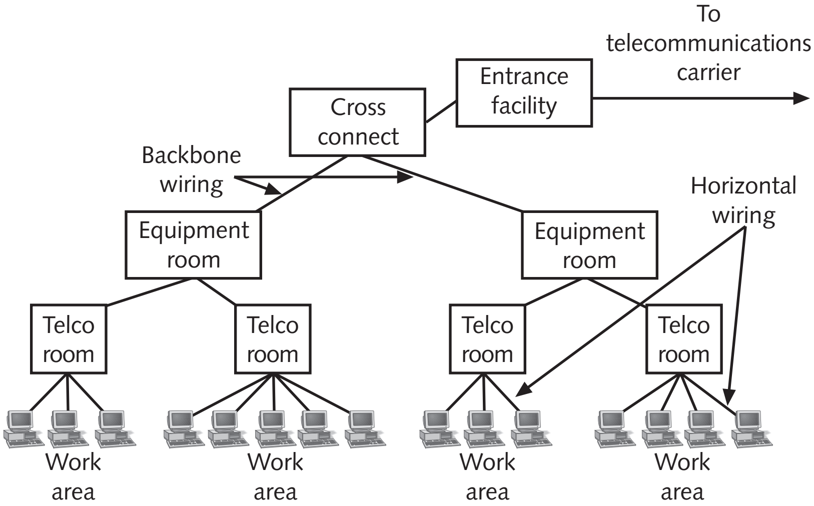

Figure 4-35 A structured cabling hierarchy

Adhering to standard cabling hierarchies is only part of a smart cable management strategy. You or your network manager should also specify standards for the types of cable used by your organization and maintain a list of approved cabling vendors. Keep a supply room stocked with spare parts so that you can easily and quickly replace defective parts.

Create documentation for your cabling plant, including the locations, lengths, and grades of installed cable. Label every data jack, punch-down block, and connector. Use color-coded cables for different purposes (cables can be purchased in a variety of sheath colors). For example, you might want to use pink for patch cables, green for horizontal wiring, and gray for vertical (backbone) wiring. Keep your documentation in a centrally accessible location and be certain to update it as you change the network. The more you document, the easier it will be to move or add cable segments.

Finally, plan for how your cabling plant will lend itself to growth. For example, if your organization is rapidly expanding, consider replacing your backbone with fiber and leave plenty of space in your telecommunications closets for more racks.

As you will most likely work with twisted-pair cable, the next section explains how to install this type of cabling from the server to the desktop.

INSTALLING CABLE

So far, you have read about the variety of cables used in networking and the limitations inherent in each. You may worry that with hundreds of varieties of cable, choosing the correct one and making it work with your network is next to impossible. The good news is that if you follow both the manufacturers' installation guidelines and the TIA/EIA standards, you are almost guaranteed success. Many network problems can be traced to poor cable installation techniques. For example, if you don't crimp twisted-pair wires in the correct position in an RJ-45 connector, the cable will fail to transmit or receive data (or both—in which case, the cable will not function at all). Installing the wrong grade of cable can either cause your network to fail or render it more susceptible to damage (for example, using typical, inexpensive twisted-pair cable in areas that might be susceptible to fire damage).

With networks moving to faster transmission speeds, adhering to installation guidelines is a more critical concern than ever. A Category 5 UTP segment that flawlessly transmits data at 10 Mbps may suffer data loss when pushed to 100 Mbps. In addition, some cable manufacturers will not honor warranties if their cables were improperly installed. This section outlines the most common method of installing UTP cable and points out cabling mistakes that can lead to network instability.

In the previous section, you learned about the six subsystems of the TIA/EIA structured cabling standard. A typical UTP network uses a modular setup to distinguish between cables at each subsystem. Figure 4-36 provides an overview of a modular cabling installation.

In this example, patch cables connect network devices (such as a workstation) to the wall jacks. Longer cables connect wire from the wall jack to a punch-down block in the telecommunications closet. From the punch-down block, patch cables bring the connection into a patch panel. From the patch panel, more patch cables connect to the hub or switch, which in turn connects to the equipment room or to the backbone, depending on the scale of the network. All of these sections of cable make network moves and additions easier. Believe it or not, they also keep the telecommunications closet organized.

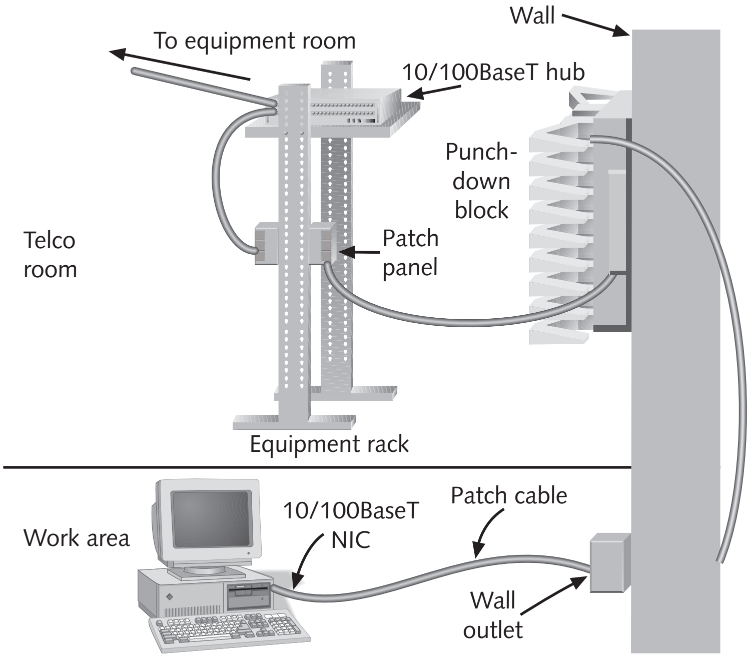

Figure 4-36 A typical UTP cabling installation

Although you may never have to make your own patch cables, you might have to repair one in a pinch. Table 4-5 explains how the pins in an RJ-45 connector correspond to the wires in a UTP cable. For example, in wire pair number 2, the green and the green and white striped wires are wound around each other. In this pair, the green wire transmits data from the device, while the green and white striped wire receives data from the network. The method of UTP coding described in Table 4-5 follows the TIA/EIA T568A wiring standard, the most popular wiring standard currently in use for networks. Another standard, the TIA/EIA T568B standard, is similar but the wire pairs colored orange and orange striped plus green and green striped are reversed. Yet another coding scheme has been established by IEEE. It typically doesn't matter which scheme you choose, but to avoid confusion and potential transmission errors you should ensure that you cable all wiring on your LAN according to one standard. In Project 4-2 at the end of this chapter, you will have the opportunity to create your own patch cable following these guidelines. Be advised, however, that any imperfection in how you fasten the wires in the connector will prevent the cable from working.

Table 4-5 Pin numbers and color codes for an RJ-45 connector

Pin Number	Pair Number	Use	Color
1	2	Transmit	White with green stripe
2	2	Receive	Green
3	3	Transmit	White with orange stripe
4	1	Receive	Blue
5	1	Transmit	White with blue stripe
6	3	Receive	Orange
7	4	Transmit	White with brown stripe
8	4	Receive	Brown

The type of patch cable detailed above is called a **straight-through cable**, so named because the terminations at both ends are identical, allowing the wires to pass "straight through." However, in some cases you may want to change the pin locations of some wires. One example is when you want to connect two network devices without using a connectivity device. This can be accomplished through the use of a **crossover cable**, a patch cable in which the terminations locations of the transmit and receive wires on one end of the cable are reversed, as shown in Figure 4-37. (Note that in the figure, T equals Transmit and R equals Receive.) Crossover cables can be useful in troubleshooting network problems when you suspect that a single device's networking hardware or software might be at fault.

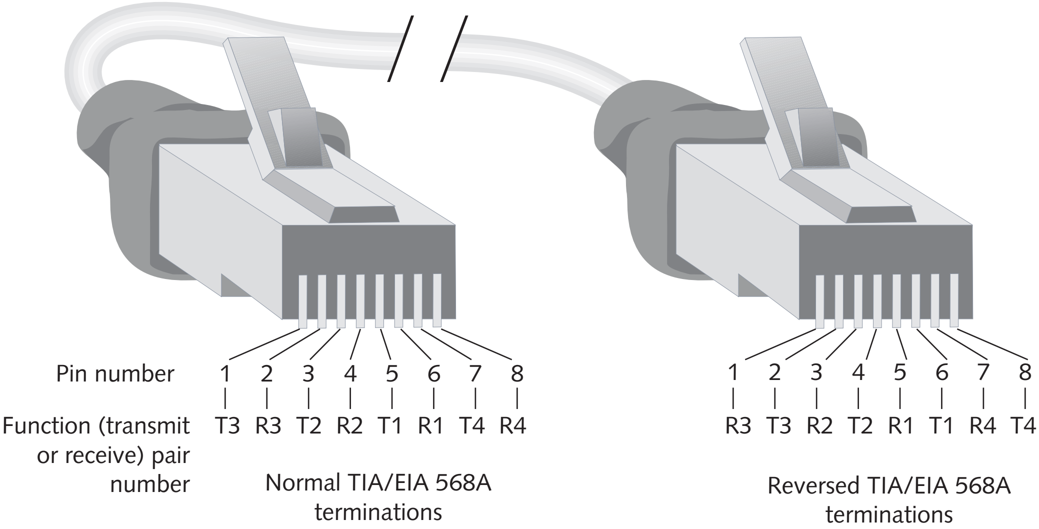
Pin number
1 2 3 4 5 6 7 8
Function (transmit or receive) pair number
T3 R3 T2 R2 T1 R1 T4 R4
Normal TIA/EIA 568A terminations
1 2 3 4 5 6 7 8
R3 T3 R2 T2 R1 T1 R4 T4
Reversed TIA/EIA 568A terminations

Figure 4-37 RJ-45 terminations on a crossover

The art of proper cabling could fill an entire book. If you plan to specialize in cable installation, design, or maintenance, you should invest in a reference dedicated to this topic. As a network professional, you will likely occasionally add new cables to a room or telecommunications closet, repair defective cable ends, or install a data outlet. Following are some cable installation tips that will help prevent Physical layer failures:

- Do not untwist twisted-pair cables more than one-half inch before inserting them into the punch-down block.
- Do not strip off more than 1 inch of insulation from the copper wire in twisted-pair cables.
- Pay attention to the bend radius limitations for the type of cable you are installing. **Bend radius** is the radius of the maximum arc into which you can loop a cable before you will impair data transmission. Generally, a twisted-pair cable's bend radius is equal to or greater than four times the diameter of the cable. Be careful not to exceed it.
- Test each segment of cabling as you install it with a cable tester. This practice will prevent you from later having to track down errors in multiple, long stretches of cable.
- Use only cable ties to cinch groups of cables together. In addition, avoid cinching cables so tightly that you squeeze their outer covering, a practice that leads to difficult-to-diagnose data errors.
- Avoid laying cable across the floor where it might sustain damage from rolling chairs or foot traffic. If you must take this tack, cover the cable with a cable protector.
- Install cable at least 3 feet away from fluorescent lights or other sources of EMI.
- Always leave slack in cable runs. Stringing cable too tightly risks connectivity and data transmission problems.
- If you run cable in the **plenum**, the area above the ceiling tile or below the subflooring, make sure the cable sheath is plenum-rated and consult with local electric installation codes to be certain you are installing it correctly. A plenum-rated cable is more fire-resistant than other cables, and its sheath will not release noxious fumes if it does start to burn.
- Pay attention to grounding requirements and follow them religiously.

Tip

Do not lay cable where animals or children can access it. Cases of squirrels or rabbits chewing through UTP are more common than you might think.

Atmospheric Transmission Media

The earth's atmosphere provides an intangible means of transporting data over networks. For decades, radio and TV stations have used the atmosphere to transport information via analog signals. The atmosphere is also capable of carrying digital signals. Networks that transmit signals through the atmosphere are known as **wireless** networks. Wireless LANs typically use infrared or radiofrequency (RF) signaling. These transmission media are suited to very specialized network environments. For example, inventory control personnel who drive through large warehouses to record inventory data benefit from the mobility of wireless networking. In addition to infrared and RF transmission, microwave and satellite links can be used to transport data through the atmosphere.

Infrared Transmission

Infrared networks use infrared light signals to transmit data through space, not unlike the way a television remote control sends signals across the room. Networks may use two types of infrared transmission: direct or indirect.

Direct infrared transmission depends on the transmitter and receiver remaining within the line of sight of each other. Just as you cannot switch TV channels with your remote control from behind a wall, so you cannot transmit data through direct infrared between two computers that don't have a clear atmospheric path between them. This "line of sight" limitation prevents widespread use of direct infrared in modern networking environments. On the other hand, the same requirement makes direct infrared more secure than many other transmission methods. When signals are limited to a specific pathway, they become difficult to intercept.

Currently, direct infrared transmission is most often used for communications between devices in the same room. For example, wireless printer connections use direct infrared transmission, as do some synchronizing features of palmtop PCs. Infrared ports are almost standard on business laptop PCs. Many desktop PCs also come equipped with infrared ports.

In **indirect infrared transmission**, signals bounce off walls, ceilings, and any other objects in their path. Because indirect infrared signals are not confined to a specific pathway, this means of transmitting data is not very secure.

Infrared pathways can carry data at rates that rival fiber-optic cable's throughput. Infrared has been proven to function at 100 Mbps, but could probably carry even more traffic. It can span distances up to 1000 m, which is nearly as far as multimode fiber.

RF Transmission

Radiofrequency (RF) transmission relies on signals broadcast over specific frequencies, in the same manner as radio and TV broadcasts. At certain frequencies, RF can penetrate walls, making it the best wireless solution for networks that must transmit data through or around walls, ceilings, and other obstacles. This same characteristic permits easy interception of most types of RF transmissions. Therefore, RF should not be used in environments where data security is important.

In addition, RF is very susceptible to interference and, therefore, would not be a good medium for EMI-saturated locations such as factory floors. Because RF signals can easily interfere with each other, frequencies must be licensed from the Federal Communications Commission (FCC). Neither the frequency nor the geographic location where the frequency is transmitted can be altered without violating the terms of the license. Makers of RF computer and networking components must, therefore, obtain licenses for specific frequencies in different geographic locations. The licensing procedure ensures that nearby systems will not operate at the same frequencies and interfere with each other's signals.

The two most common RF technologies are **narrowband**, which concentrates significant RF energy at a single frequency, and **spread spectrum**, which uses a lower-level signal distributed over several frequencies simultaneously. Although narrowband RF can be easily intercepted and is, therefore, not suited for sensitive data transfer, spread spectrum RF is quite secure. Both types of RF offer a moderate throughput, ranging as high as 10 Mbps.

Note

The U.S. Navy uses spread spectrum RF networking in a most intriguing way. Its ships travel in groups and communicate with each other across the water using RF and satellite network links. Because their transmissions must remain secure, they use spread spectrum RF rather than narrowband RF.

Choosing the Right Transmission Medium

Now that you have read about the characteristics, benefits, and disadvantages of all types of network transmission media, you need to consider how to evaluate them in terms of realistic network environments. The following list summarizes the majority of environmental factors you must take into account and suggests appropriate transmission media for the various conditions. Most environments will contain a combination of these factors; you must therefore weigh the significance of each against the cost of your optimal solution.

- *Areas of high EMI or RFI*—If the environment houses a number of electrical power sources, you will want to use the most noise-resistant medium possible. Thick Ethernet and fiber-optic cable are the most noise-resistant media currently available.
- *Corners and small spaces*—If the environment requires that cable bend around tight corners or through small spaces, you should use the most flexible medium possible. STP and UTP are both very flexible.
- *Distance*—If the environment requires long stretches of transmission, you might want to consider fiber-optic or wireless media. You can use twisted-pair and coaxial media, but they are more susceptible to attenuation and interference and will require the use of repeaters.
- *Security*—If your organization is concerned about wire taps, you will want to choose the transmission media with the highest security. Fiber-optic, direct infrared, and spread spectrum RF media are excellent choices for this environment.
- *Existing infrastructure*—If you are adding cable to an existing cable plant, you will need to consider how it will interact with existing cabling and

connectivity hardware. The media you choose should be tailored to your organization's previously installed equipment.

- *Growth*—Find out how your organization plans to expand its network and consider future applications, traffic, and geographic expansion when designing its cable plant. In this instance, the medium you choose should be tailored to your organization's needs.

Chapter Summary

- ❐ Information can be transmitted via two methods: analog or digital. Analog signals are continuous waves that result in variable and inexact transmission. Digital signals are based on electrical or light pulses that represent information encoded in binary form.
- ❐ In half-duplex transmission, signals may travel in both directions over a medium but in only one direction at a time. When signals may travel in both directions over a medium simultaneously, the transmission is considered full-duplex.
- ❐ A form of transmission that allows multiple signals to simultaneously travel over one medium is known as multiplexing. In multiplexing, the single medium is logically separated into multiple channels, or subchannels.
- ❐ Throughput is the amount of data that the medium can transmit during a given period of time. Throughput is usually measured in bits per second. The physical nature of every transmission medium determines its potential throughput.
- ❐ Baseband is a form of transmission in which digital signals are sent through direct current pulses applied to the wire. Baseband systems can transmit only one signal, or one channel, at a time. Broadband, on the other hand, uses modulated analog frequencies to transmit multiple signals over the same wire.
- ❐ Noise is interference that distorts an analog or digital signal. It may be caused by electrical sources, such as power lines, fluorescent lights, copiers, and microwave ovens, or by broadcast signals.
- ❐ Analog and digital signals both suffer attenuation, or loss of signal, as they travel farther from their sources. To compensate, analog signals are amplified, and digital signals are regenerated through repeaters. Digital signals can be regenerated without any noise they might have accumulated; analog signals, on the other hand, are amplified along with the accompanying noise.
- ❐ When considering media cost, you must calculate not only the cost of the physical medium, but also the cost of installation, connectivity hardware, maintenance, obsolescence, and productivity gained or lost as a result of a medium's capacity.
- ❐ Three specifications dictate the size and scalability of networking media: maximum nodes per segment, maximum segment length, and maximum network length.
- ❐ After a certain distance, a signal attenuates so much that it cannot be accurately interpreted. Thus, a repeater on the network must retransmit and amplify the signal. The

maximum distance that a signal can travel and still be accurately interpreted equals the maximum segment length.

- Every network is susceptible to a delay between the transmission of a signal and its receipt. This delay is called latency. The length of the cable contributes to latency, as does the presence of any intervening connectivity device, such as a router.
- Connectors are the pieces of hardware that connect the wire to the network device, be it a file server, workstation, switch, or printer. Every networking medium requires a specific kind of connector.
- Coaxial cable consists of a central copper core surrounded by a plastic insulator, a braided metal shielding called braiding, and an outer plastic cover called the sheath. The copper core carries the electromagnetic signal, and the braiding acts as both a shield against noise and a ground for the signal. The insulator layer protects the copper core from the metal shielding. The sheath protects the cable from physical damage.
- Thicknet cabling, also called thickwire Ethernet, is a rigid coaxial cable approximately 1 cm thick that was used for the original Ethernet networks. IEEE has designated Thicknet as 10Base5 Ethernet. The "10" represents its throughput of 10 Mbps, the "Base" stands for baseband transmission, and the "5" represents the maximum segment length of a Thicknet cable, 500 m.
- Most Thicknet networks use AUI (also known as DB-15 or DIX) connectors on drop cables to connect network nodes to transceivers known as MAUs (media access units).
- Thinnet, also known as Thin Ethernet, or 10Base2 was the most popular medium for Ethernet LANs in the 1980s, but is rarely used on modern networks. The "10" represents its data transmission rate of 10 Mbps, "Base" represents the fact that it uses baseband transmission, and the "2" represents its maximum segment length of 185 m (roughly 200 m). Thinnet is easier to handle and install than Thicknet, but provides less resistance to noise.
- Thinnet uses BNC connectors between the network backbone, drop cables, and network nodes.
- Both Thicknet and Thinnet coaxial cable rely on the bus topology and must be terminated at both ends with a resistor to prevent signal bounce. Thicknet and Thinnet cable must also be grounded at one end.
- Twisted-pair cable consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm, twisted around each other and encased in plastic coating. The twists in the wire help to reduce the effects of crosstalk.
- Shielded twisted-pair (STP) cable consists of twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil, to reduce the effects of noise on the signal.
- Unshielded twisted-pair (UTP) cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name suggests, UTP does not contain additional

shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP.

- UTP comes in a variety of specifications, including CAT1 through CAT7, as specified by the TIA/EIA 568 standard. You will probably encounter CAT5 or CAT5e on contemporary LANs.
- CAT3 is a form of UTP that contains four wire pairs and can carry data at a rate as high as 10 Mbps, with a possible bandwidth of 16 MHz. CAT3 has typically been used for 10-Mbps Ethernet or 4-Mbps Token Ring networks.
- CAT5 and CAT5e are the most popular form of UTP for new network installations and upgrades to Fast Ethernet. CAT5 contains four wire pairs and supports up to 100-Mbps throughput and a 100-MHz signal rate. In addition to 100-Mbps Ethernet, CAT5 wiring can support other fast networking technologies.
- 10BaseT is a physical specification for an Ethernet network that is capable of 10-Mbps throughput and uses baseband transmission and twisted-pair media. It has a maximum segment length of 100 meters.
- 100BaseT is a physical specification for an Ethernet network that is capable of 100-Mbps throughput and uses baseband transmission and twisted-pair media.
- Two types of 100BaseT exist: 100BaseTX, which uses only two wire pairs, and 100BaseT4, which uses all four wire pairs in the cable. 100BaseTX is capable of full duplexing while 100BaseT4 can only achieve half duplexing and also requires different connectivity equipment than 10BaseT or 100BaseTX. 100BaseT may also be called "Fast Ethernet."
- Fiber-optic cable contains one or several glass fibers in its core. Data are transmitted via pulsing light sent from a laser or light-emitting diode through the central fiber(s). Outside the fiber(s), a layer of glass called cladding acts as a mirror, reflecting light back to the core in different patterns that vary depending on the transmission mode. Outside the cladding, a plastic buffer and strands of Kevlar protect the inner core. A plastic sheath covers the braiding.
- Fiber cable variations fall into two categories: single-mode and multimode. Single-mode fiber uses a small-diameter core, over which light generated by a laser travels mostly down its center, reflecting very few times. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows single-mode fiber to accommodate high bandwidths and long distances (without requiring repeaters).
- Multimode fiber uses a core with a larger diameter, over which many pulses of light generated by a light emitting diode (LED) travel at different angles. Because light is being reflected many different ways in a multimode fiber cable, the waves become less easily distinguishable the longer they travel.
- On today's networks, fiber is used primarily as a backbone cable. Fiber-optic cable provides the benefits of very high throughput, very high resistance to noise, and excellent security.

- 10BaseF is a Physical layer specification for a network that can achieve 10-Mbps throughput using baseband transmission and running on multimode fiber. Depending on the version, 10BaseF networks may have a maximum segment length of 1000 or 2000 meters.
- 100BaseF is a Physical layer specification for a network that can achieve 100-Mbps throughput using baseband transmission running on multimode fiber. Its maximum segment length is 400 meters. It may also be called "Fast Ethernet."
- In 1991, TIA/EIA released their joint 568 Commercial Building Wiring Standard, also known as structured cabling, for uniform, enterprise-wide, multivendor cabling systems. Structured cabling is based on a hierarchical design that divides cabling into six subsystems: entrance facility, backbone (vertical) wiring, equipment room, telecommunications closet, horizontal wiring, and work area.
- The best practice for installing cable is to follow the TIA/EIA 568 specifications and the manufacturer's recommendations. Be careful not to exceed a cable's bend radius, untwist wire pairs more than one-half inch, or remove more than 1 inch of insulation from copper wire. Install plenum-rated cable in ceilings and floors, and run cabling far from where it might suffer physical damage.
- Wireless LANs can use either radiofrequency (RF) or infrared transmission. Wireless transmission is typically used in very specialized applications, often to facilitate mobile computing.
- Infrared transmission comes in two main flavors: indirect infrared and direct infrared. Indirect infrared signals bounce off ceilings, walls, and any other obstacles between the sender and receiver. Direct infrared signals require that the sender and receiver establish an unobstructed path through the air.
- RF transmission also comes in two flavors: narrowband and spread spectrum. Narrowband RF uses a single frequency and can be easily intercepted and decoded. Spread spectrum RF distributes the signals over several frequencies and is difficult to intercept.
- To determine which transmission media are right for a particular networking environment, you must consider the organization's required throughput, cabling distance, noise resistance, security, flexibility, and plans for growth.

KEY TERMS

1 gigabit per second (Gbps) — 1,000,000,000 bits per second.

1 kilobit per second (Kbps) — 1000 bits per second.

1 megabit per second (Mbps) — 1,000,000 bits per second.

1 terabit per second (Tbps) — 1,000,000,000 bits per second.

10Base2 — See *Thinnet.*

10Base5 — See *Thicknet.*

10BaseF — A Physical layer standard for networks that specifies baseband transmission, multimode fiber cabling, and 10-Mbps throughput. 10BaseF networks have a maximum segment length of 1000 or 2000 meters, depending on the version, and employ a star topology.

10BaseT — A Physical layer standard for networks that specifies baseband transmission, twisted pair media, and 10-Mbps throughput. 10BaseT networks have a maximum segment length of 100 meters and rely on a star topology.

100BaseFX — A Physical layer standard for networks that specifies baseband transmission, multimode fiber cabling, and 100-Mbps throughput. 100BaseFX networks have a maximum segment length of 400 meters. 100BaseFX may also be called "Fast Ethernet."

100BaseT — A Physical layer standard for networks that specifies baseband transmission, twisted-pair cabling, and 100-Mbps throughput. 100BaseT networks have a maximum segment length of 100 meters and use the star topology. 100BaseT is also known as Fast Ethernet.

100BaseT4 — A type of 100BaseT network that uses all four wire pairs in a twisted-pair cable to achieve its 100-Mbps throughput. 100BaseT4 is not capable of full-duplex transmission and requires CAT3 or higher media.

100BaseTX — A type of 100BaseT network that uses two wire pairs in a twisted-pair cable, but uses faster signaling to achieve 100-Mbps throughput. It is capable of full-duplex transmission and requires CAT5 or higher media.

100BaseVG (100VG-AnyLAN) — A Physical layer standard for networks that specifies baseband transmission, twisted-pair media, and 100-Mbps throughput. 100BaseVG uses a different and more efficient method than 100BaseT for allowing nodes to transmit data on the media. However, 100BaseVG is rarely used.

alien crosstalk — A type of interference that occurs when signals from an adjacent cable interfere with another cable's transmission.

amplifier — A device that boosts, or strengthens, an analog signal.

amplitude — A measure of a signal's strength.

amplitude modulation (AM) — A modulation technique in which the amplitude of the carrier signal is modified by the application of a data signal.

analog — A signal that uses variable voltage to create continuous waves, resulting in an inexact transmission.

attenuate — To lose signal strength as a transmission travels farther away from its source.

attenuation — The amount of signal loss over a given distance.

AUI (Attachment Unit Interface) — An Ethernet standard for connecting coaxial cables with transceivers and networked nodes.

backbone — A network of networks. Backbone wiring provides interconnection between telecommunications closets, equipment rooms, and entrance facilities.

bandwidth — A measure of the difference between the highest and lowest frequencies that a medium can transmit.

baseband — A form of transmission in which digital signals are sent through direct current pulses applied to the wire. This direct current requires exclusive use of the wire's capacity, so baseband systems can transmit only one signal, or one channel, at a time. Every device on a baseband system shares a single channel.

bend radius — The radius of the maximum arc into which you can loop a cable before you will cause data transmission errors. Generally, a twisted-pair cable's bend radius is equal to or greater than four times the diameter of the cable.

binary — A system founded on using 1s and 0s to encode information.

bit — Short for binary digit. A bit equals a single pulse in the digital encoding system. It may have only one of two values: 0 or 1.

BNC barrel connector — A connector used on Thinnet networks with two open ends used to connect two Thinnet coaxial cables.

BNC T-connector — A connector used on Thinnet networks with three open ends. It attaches to the Ethernet interface card at the base of the "T" and to the Thinnet cable at its two sides so as to allow the signal in and out of the NIC.

braiding — A braided metal shielding used to insulate some types of coaxial cable.

broadband — A form of transmission in which signals are modulated as radiofrequency analog pulses with different frequency ranges. Unlike baseband, broadband technology does not involve binary encoding. The use of multiple frequencies enables a broadband system to operate over several channels and therefore carry much more data than a baseband system.

broadcast — A transmission that involves one transmitter and multiple receivers.

byte — Eight bits of information. In a digital signaling system, broadly speaking, one byte carries one piece of information.

cable plant — The hardware that constitutes the enterprise-wide cabling system.

capacity — See *throughput.*

CAT — Abbreviation for the word "category" when describing a type of twisted-pair cable. For example, Category 3 unsheilded twisted-pair cable may also be called CAT3. See *Category 1, Category 2, Category 3, Category 4, Category 5, Enhanced Category 5, Category 6,* and *Category 7.*

Category 1 (CAT1) — A form of UTP that contains two wire pairs. CAT1 is suitable for voice communications, but not for data. At most, it can carry only 20 Kbps of data.

Category 2 (CAT2) — A form of UTP that contains four wire pairs and can carry up to 4 Mbps of data. CAT2 is rarely found on modern networks, because most require higher throughput.

Category 3 (CAT3) — A form of UTP that contains four wire pairs and can carry up to 10-Mbps, with a possible bandwidth of 16 MHz. CAT3 has typically been used for 10-Mbps Ethernet or 4-Mbps Token Ring networks. Network administrators are gradually replacing CAT3 cabling with CAT5 to accommodate higher throughput. CAT3 is less expensive than CAT5.

Category 4 (CAT4) — A form of UTP that contains four wire pairs and can support up to 16-Mbps throughput. CAT4 may be used for 16-Mbps Token Ring or 10-Mbps Ethernet networks. It is guaranteed for data transmission up to 20 MHz and provides more protection against crosstalk and attenuation than CAT1, CAT2, or CAT3.

Category 5 (CAT5) — The most popular form of UTP for new network installations and upgrades to Fast Ethernet. CAT5 contains four wire pairs and supports up to 100-Mbps throughput and a 100 MHz signal rate. In addition to 100-Mbps Ethernet, CAT5 wiring can support other fast networking technologies, such as Asynchronous Transfer Mode (ATM) and Fiber Distributed Data Interface (FDDI).

Category 6 (CAT6) — A twisted-pair cable that contains four wire pairs, each wrapped in foil insulation. Additional foil insulation covers the bundle of wire pairs, and a fire-resistant plastic sheath covers the second foil layer. The foil insulation provides excellent resistance to crosstalk and enables CAT6 to support at least six times the throughput supported by regular CAT5.

Category 7 (CAT7) — A twisted-pair cable that contains multiple wire pairs, each separately shielded then surrounded by another layer of shielding within the jacket. CAT7 can support up to a 1-GHz signal rate. But because of its extra layers, it is less flexible than other forms of twisted-pair wiring.

channel — A distinct communication path between two or more nodes, much like a lane is a distinct transportation path on a freeway. Channels may be separated either logically (as in multiplexing) or physically (as when they are carried by separate wires).

cladding — The glass shield around the fiber core of a fiber-optic cable. Cladding acts as a mirror, reflecting light back to the core in patterns that vary depending on the transmission mode. This reflection allows fiber to bend around corners without impairing the light-based signal.

coaxial cable — A type of cable that consists of a central copper core surrounded by an insulator, a braided metal shielding, called braiding, and an outer cover, called the sheath or jacket. Coaxial cable, called "coax" for short, was the foundation for Ethernet networks in the 1980s and remained a popular transmission medium for many years.

conduit — Pipeline used to contain and protect the cabling. Conduit is usually made from metal.

connectors — The pieces of hardware that connect the wire to the network device, be it a file server, workstation, switch, or printer.

core — The central component of a fiber-optic cable, consisting of one or several pure glass fibers.

crossover cable — A twisted-pair patch cable in which the termination locations of the transmit and receive wires on one end of the cable are reversed.

crosstalk — A type of interference caused by signals traveling on nearby wire pairs infringing on another pair's signal.

DB-15 — A general term for connectors that use 15 metal pins to complete a connection between devices. "DB" stands for Data bus, while the number "15" indicates how many pins are used to make the connection.

demultiplexer (demux) — A device that separates multiplexed signals once they are received and regenerates them in their original form.

digital — As opposed to analog signals, digital signals are composed of pulses that can have a value of only 1 or 0.

direct infrared transmission — A type of infrared transmission that depends on the transmitter and receiver being within the line of sight of each other.

DIX (Digital, Intel, and Xerox) — A type of AUI connector used on Thicknet networks.

drop cable — The cable that connects a device's Ethernet interface to a transceiver in a Thicknet network.

duplex — See *full-duplex*.

electromagnetic interference (EMI) — A type of interference that may be caused by motors, power lines, televisions, copiers, fluorescent lights, or other sources of electrical activity.

enhanced CAT5 (CAT5e) — A higher-grade version of CAT5 wiring that contains high-quality copper, offers a high twist ratio, and uses advanced methods for reducing crosstalk. Enhanced CAT5 can support a signaling rate of up to 200 MHz, double the capability of regular CAT5.

enterprise-wide network — A network that spans an entire organization and often services the needs of many diverse users. It may include many locations (as a WAN), or it may be confined to one location but include many different departments, floors, and network segments.

Fast Ethernet — A type of Ethernet network that is capable of 100-Mbps throughput. 100BaseT and 100BaseFX are both examples of Fast Ethernet.

fiber-optic cable — A form of cable that contains one or several glass fibers in its core. Data are transmitted via pulsing light sent from a laser or light-emitting diode through the central fiber (or fibers). Outside the central fiber, a layer of glass called cladding acts as a mirror, reflecting light back to the core in patterns that vary depending on the transmission mode. Outside the cladding, a plastic buffer protects the core and absorbs any light that might escape. Outside the buffer, strands of Kevlar provide further protection from stretching and damage. A plastic jacket surrounds the Kevlar strands.

fiber-optic modem (FOM) — A demultiplexer used on fiber networks that employ wave division multiplexing. The fiber-optic modem separates the multiplexed signals into individual signals according to their different wavelengths.

frequency — The number of times that a signal's amplitude changes over a fixed period of time, expressed in cycles per second, or hertz (Hz).

frequency modulation (FM) — A method of data modulation in which the frequency of the carrier signal is modified by the application of the data signal.

full-duplex — A type of transmission in which signals may travel in both directions over a medium simultaneously. May also be called, simply, "duplex."

half-duplex — A type of transmission in which signals may travel in both directions over a medium, but in only one direction at a time.

hertz (Hz) — A measure of frequency equivalent to the number of amplitude cycles per second.

indirect infrared transmission — A type of infrared transmission in which signals bounce off walls, ceilings, and any other objects in their path. Because indirect infrared signals are not confined to a specific pathway, they are not very secure.

infrared — A type of data transmission in which infrared light signals are used to transmit data through space, similar to the way a television remote control sends signals across the room. Networks may use two types of infrared transmission: direct or indirect.

latency — The delay between the transmission of a signal and its receipt.

media access unit (MAU) — The type of transceiver used on a Thicknet network to connect network nodes to the backbone.

modem — A device that modulates analog signals into digital signals at the transmitting end for transmission over telephone lines, and demodulates digital signals into analog signals at the receiving end.

modulation — A technique for formatting signals in which one property of a simple, carrier wave is modified by the addition of a data signal during transmission.

multimode fiber — A type of fiber-optic cable that contains a core with a diameter between 50 and 100 microns, over which many pulses of light generated by a light emitting diode (LED) travel at different angles. Because light is being reflected many different ways in a multimode fiber cable, the waves become less easily distinguishable the longer they travel. Thus, multimode fiber is best suited for shorter distances than single-mode fiber.

multiplexer (mux) — A device that separates a medium into multiple channels and issues signals to each of those subchannels.

multiplexing — A form of transmission that allows multiple signals to simultaneously travel over one medium.

n-series connector (n connector) — A type of connector used on Thicknet networks in which a screw-and-barrel arrangement securely connects coaxial cables to devices.

narrowband — A type of radiofrequency transmission in which signals travel over a single frequency. The same method is used by radio and TV broadcasting stations, and signals can be easily intercepted and decoded.

noise — Unwanted signals, or interference, from sources near network cabling, such as electrical motors, power lines and radar.

optical loss — The degradation of a light signal on a fiber-optic network.

overhead — The nondata information that must accompany data in order for a signal to be properly routed and interpreted by the network.

patch cable — A relatively short section (usually between 3 and 50 feet) of twisted-pair cabling, with connectors on both ends, that connects network devices to data outlets.

patch panel — A wall-mounted panel of data receptors into which cross-connect patch cables from the punch-down block are inserted.

phase — A point or stage in a wave's progress over time.

plenum — The area above the ceiling tile or below the subfloor in a building.

point-to-point — A data transmission that involves one transmitter and one receiver.

punch-down block — A panel of data receptors into which horizontal cabling from the workstations is inserted.

radiofrequency (RF) — A type of transmission that relies on signals broadcast over specific frequencies, in the same manner as radio and TV broadcasts. RF may use narrowband or spread spectrum technology.

radiofrequency interference (RFI) — A kind of interference that may be generated by motors, power lines, televisions, copiers, fluorescent lights, or broadcast signals from radio or TV towers.

regeneration — The process of retransmitting a digital signal. Regeneration, unlike amplification, repeats the pure signal, with none of the noise it has accumulated.

repeater — A device used to regenerate a signal.

risers — The backbone cabling that provides vertical connections between floors of a building.

RJ-45 — The standard connector used with shielded twisted-pair and unshielded twisted-pair cabling. "RJ" stands for registered jack.

sheath — The outer cover, or jacket, of a cable.

shielded twisted-pair (STP) — A type of cable containing twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil. The shielding acts as an antenna, converting the noise into current (assuming that the wire is properly grounded). This current induces an equal, yet opposite current in the twisted pairs it surrounds. The noise on the shielding mirrors the noise on the twisted pairs, and the two cancel each other out.

signal bounce — A phenomenon caused by improper termination on a bus network in which signals travel endlessly between the two ends of the network, preventing new signals from getting through.

simplex — A type of transmission in which signals may travel in only one direction over a medium.

single-mode fiber — A type of fiber-optic cable with a narrow core that carries light pulses along a single path data from one end of the cable to the other end. Data can be transmitted faster and for longer distances on single-mode fiber than on multimode fiber. Single-mode fiber is extremely expensive.

spread spectrum — A type of radiofrequency transmission in which lower-level signals are distributed over several frequencies simultaneously. Spread spectrum RF is more secure than narrowband RF.

statistical multiplexing — A method of multiplexing in which each node on a network is assigned a separate time slot for transmission, based on the node's priority and need.

straight-through cable — A twisted-pair patch cable in which the wire terminations in both connectors follow the same scheme.

structured cabling — A method for uniform, enterprise-wide, multivendor cabling systems specified by the TIA/EIA 568 Commercial Building Wiring Standard. Structured cabling is based on a hierarchical design using a high-speed backbone.

subchannel — One of many distinct communication paths established when a channel is multiplexed or modulated.

Thicknet — A type of coaxial cable, also known as thickwire Ethernet, that is a rigid cable approximately 1-cm thick. Thicknet was used for the original Ethernet networks. Because it is often covered with a yellow sheath, Thicknet is also called "yellow Ethernet." IEEE has designated Thicknet as 10Base5 Ethernet, with the "10" representing its throughput of 10 Mbps, the "Base" standing for baseband transmission, and the "5" representing the maximum segment length of a Thicknet cable, 500 m.

thickwire Ethernet — See *Thicknet*.

thin Ethernet — See *Thinnet*.

Thinnet — A type of coaxial cable, also known as thin Ethernet, that was the most popular medium for Ethernet LANs in the 1980s. Like Thicknet, Thinnet is rarely used on modern networks. IEEE has designated Thinnet as 10Base2 Ethernet, with the "10" representing its data transmission rate of 10 Mbps, the "Base" representing the fact that it uses baseband transmission, and the "2" roughly representing its maximum segment length of 185 m.

throughput — The amount of data that a medium can transmit during a given period of time. Throughput is usually measured in megabits (1,000,000 bits) per second, or Mbps. The physical nature of every transmission media determines its potential throughput.

time division multiplexing (TDM) — A method of multiplexing that assigns a time slot in the flow of communications to every node on the network and in that time slot, carries data from that node.

transceiver (transmitter/receiver) — A device that both transmits and receives signals. Since a transceiver is concerned with applying signals to the wire, it belongs in the Physical layer of the OSI Model. Many different types of transceivers exist in networking.

transmission — In networking, the application of data signals to a medium or the progress of data signals over a medium from one point to another.

twist ratio — The number of twists per meter or foot in a twisted-pair cable.

twisted-pair (TP) — A type of cable similar to telephone wiring that consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm, twisted around each other and encased in plastic coating.

unshielded twisted-pair (UTP) — A type of cabling that consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP.

vampire tap — A connector used on Thicknet MAUs that pierces a hole in the coaxial cable, thus completing a connection between the metal tooth in the vampire tap and the copper core of the cable.

volt — Measurement used to describe the degree of pressure an electrical current exerts on a conductor.

voltage — The pressure (sometimes informally referred to as the strength) of an electrical current.

wavelength — The distance between corresponding points on a wave's cycle. Wavelength is inversely proportional to frequency.

wavelength division multiplexing (WDM) — A multiplexing technique in which each signal on a fiber-optic cable is assigned a different wavelength, which equates to its own subchannel. Each wavelength is modulated with a data signal. In this manner multiple signals can be simultaneously transmitted in the same direction over a length of fiber.

Webcasting — A broadcast transmission from one Internet-attached node to multiple other Internet-attached nodes.

wireless — Networks that transmit signals through the atmosphere via infrared or RF signaling.

REVIEW QUESTIONS

1. When they become faint, analog signals are regenerated while digital signals are amplified. True or False?
2. Which two of the following technologies cannot achieve full-duplex transmission?
   a. 10BaseT
   b. 100BaseTX
   c. 100BaseFX
   d. 100BaseT4
   e. 100BaseVG
3. What is the origin of the word "modem?"
   a. modifier/demodifier
   b. modulator/demodulator
   c. modulator/decoder
   d. multiplexer/demultiplexer
   e. moderator/demoderator
4. How does noise affect a digital signal?
   a. Noise enhances a digital signal.
   b. Noise weakens a digital signal.
   c. Noise increases the frequency of a digital signal.
   d. Noise distorts the signal.
   e. Noise does not affect digital signals.
5. Which two of the following transmission techniques can increase the potential throughput of a network?
   a. simplexing
   b. multiplexing
   c. full duplexing
   d. broadcasting
   e. amplifying

6. Which of the following would not be a source of EMI?
   a. fluorescent lighting
   b. a microwave
   c. a loud gong
   d. a cord that carries electricity to a printer
   e. a lightning storm
7. When determining the cost of a cabling system, what—besides the cost of the wire—must you bear in mind?
8. What is the term that refers to the outermost covering of a cable?
   a. cladding
   b. insulation
   c. plenum
   d. sheath
   e. braiding
9. What type of coaxial cable would you use to connect network nodes on a Thinnet network?
   a. RG-11
   b. RG-58A/U
   c. RG-59/U
   d. RG-8
   e. RG-62A/U
10. What are two advantages of using twisted-pair cabling over coaxial cabling on a network?
    a. Twisted-pair cable is more reliable.
    b. Twisted-pair cable is less expensive.
    c. Twisted-pair cable is more resistant to noise.
    d. Twisted-pair cable is more resistant to physical damage.
    e. Twisted-pair cable is required for modern transmission standards, such as 100BaseT.
11. In which of the following network types would you use a cable with AUI connectors?
    a. 10Base5
    b. 10Base2
    c. 10BaseT
    d. 10BaseF
    e. 100BaseFX
12. Describe the differences between baseband and broadband transmission.
13. What type of terminator is required at both ends of a Thinnet or Thicknet cable?
    a. 20 ohms
    b. 25 ohms

   c. 50 ohms
   d. 100 ohms
   e. 200 ohms

14. Which two of the following network types require a bus topology?
   a. 10Base5
   b. 10Base2
   c. 10BaseT
   d. 100BaseTX
   e. 100BaseVG
15. Crosstalk does not present a problem for UTP cable. True or False?
16. What is the maximum throughput currently supported by CAT5 wiring?
   a. 10 Mbps
   b. 100 Mbps
   c. 200 Mbps
   d. 1 Gbps
   e. 10 Gbps
17. How many wire pairs are in a typical CAT5 cable?
   a. 2
   b. 3
   c. 4
   d. 5
   e. 8
18. What type of fiber-optic cable is most frequently found on LANs?
   a. multithreaded fiber
   b. twisted fiber
   c. single-mode fiber
   d. braided fiber
   e. multimode fiber
19. Which two of the following are drawbacks to using fiber-optic cable for LANs?
   a. It is expensive.
   b. It cannot handle high bandwidth transmissions.
   c. It can carry transmissions using only the TCP/IP protocol.
   d. It can be difficult to install and repair.
   e. It is not yet an accepted standard for high-speed networking.
20. What is the maximum allowable distance for a horizontal wiring subsystem?
   a. 10 m
   b. 90 m

c. 100 m

d. 200 m

e. 400 m

21. What is the maximum segment length on a 100BaseT network?

a. 10 m

b. 100 m

c. 200 m

d. 400 m

e. 1000 m

22. What is the maximum segment length on a Thicknet network?

a. 50 m

b. 100 m

c. 200 m

d. 500 m

e. 1000 m

23. In what subsystem of a structured cabling design are patch cables used?

a. in the horizontal wiring

b. in the work area

c. in the backbone wiring

d. in the entrance facilities

e. on the backbone

24. What part of the TIA/EIA structured cabling recommendations provides connectivity to a telecommunications service provider?

a. work area

b. horizontal wiring

c. telecommunications closet

d. entrance facilities

e. patch panel

25. On what type of network would you use BNC connectors?

a. 10Base5

b. 10Base2

c. 10BaseT

d. 100BaseTX

e. 100BaseT4

26. On a 100BaseTX Ethernet network, where will you most likely find the transceivers?

a. in the modems

b. in the MAUs

   c. in the NICs
   d. in the horizontal cabling
   e. in the work area cabling

27. In general, what type of cabling can sustain the most bending without impairing transmission?
    a. Thinnet
    b. Thicknet
    c. STP
    d. UTP
    e. fiber-optic
28. What is the *maximum* amount of insulation you should strip from copper wires before inserting them into connectors?
    a. ¼ inch
    b. ½ inch
    c. 1 inch
    d. 2 inches
    e. 4 inches
29. What is the *maximum* amount you should untwist twisted-pair wires before inserting them into connectors?
    a. ¼ inch
    b. ½ inch
    c. 1 inch
    d. 2 inches
    e. 4 inches
30. On a 10BaseT network, which of the following best describes how the wires of a UTP cable are used to transmit and receive information?
    a. One wire pair handles data transmission, while another wire pair handles data reception.
    b. One wire in one pair handles data transmission, while the other wire in that pair handles data reception.
    c. Three wires of two wire pairs handle both data transmission and reception, while the fourth wire acts as a ground.
    d. All four wires of two wire pairs handle both data transmission and reception.
31. If you wanted to allow two workstations to transmit and receive data between their NICs without using a connectivity device, which of the following would you need?
    a. crossover cable
    b. straight-through cable
    c. AUI cable

d. DIX cable

e. Multimode cable

32. What are the two main types of infrared transmission, and how do they differ?

33. Radiofrequency transmissions can be easily intercepted. True or False?

34. What kind of transmission media is best suited to videoconferencing between two buildings that are across the street from each other?

    a. coaxial cable

    b. fiber-optic cable

    c. STP

    d. CAT5 UTP

    e. infrared

35. Which government agency in the United States allocates radio frequencies?

    a. FTA

    b. FTC

    c. SEC

    d. CCC

    e. FCC

HANDS-ON PROJECTS

Project 4-1

One of the characteristics that you must consider when choosing the right type of cable for your network is its bend radius. Bending a cable may affect its ability to transmit data. When you bend a cable past its maximum bend radius, data errors may occur. In this exercise, you will attempt to impair the transmission of data over a Thinnet coaxial cable by bending it past its maximum bend radius.

For this project, you will need a Windows 98 or 2000 Professional workstation connected to a Windows 2000 or NetWare server via Thinnet coaxial cable. You will also need a compass and a tape measure. In the first five steps of this project, you will create a continuously looping batch file, called "dirtest.bat," that repeatedly lists the contents of one directory on the server. The purpose of this batch file is to generate a steady flow of traffic between the server and your workstation.

1. At the Windows 98 or 2000 workstation, click **Start**, point to **Programs**, point to **Accessories**, and then click **Notepad**. The Notepad window opens.

2. Type the following three lines in the open document:

```
:TEST
dir /s
goto TEST
```

3. Click **File** on the menu bar, then click **Save**. The Save As dialog box opens.
4. Save the file as **dirtest.bat** in the root directory of the C: drive.
5. Close Notepad.
6. If you are using a Windows 98 workstation, click **Start**, point to **Programs**, then click **MS-DOS Prompt**. If you are using a Windows 2000 workstation, click **Start**, point to **Programs**, point to **Accessories**, then click the **Command Prompt**.
7. At the DOS prompt type **cd\** to make sure you are in the root directory.
8. At the DOS prompt, type **dirtest**. The batch file runs. You should see a directory listing continually scrolling down the screen.
9. While watching the DOS window, take a 4-foot section of the coaxial cable in your hands and slowly bend it as if you were trying to create a circle. At what point does the traffic between the workstation and the server slow down? At what point does it stop, if ever?
10. Using the compass, measure the bend radius of the cable when you notice that the transmission begins to slow down, and again when you notice that it stops.
11. After completing the exercise, close the Command Prompt (or MS-DOS) window.

Hands-on Project

Project 4-2

You may sometimes need to create your own patch cables or install a new connector on an existing cable. In this exercise, you will practice putting an RJ-45 connector on a twisted-pair cable, and then use the cable to connect a workstation to the network. The process of inserting wires into the connector is called crimping, and it is a skill that requires practice—so don't be discouraged if the first cable you create doesn't reliably transmit and receive data.

For this project, you will need a crimping tool, a wire stripper, a wire cutter, a 5-foot length of CAT5 UTP, two RJ-45 connectors, and a simple client/server network (for example, a Windows 98 or Windows 2000 Professional workstation connected to wall jack or hub as part of a Windows 2000 server network) that you have verified works with a reliable twisted-pair cable.

1. Using the wire cutter, make a clean cut at both ends of the UTP cable.
2. Using the wire stripper, remove the sheath off 1 inch (or less) of one end of the UTP cable, being careful to not damage the insulation on the twisted pairs inside.
3. Separate the four wire pairs slightly while keeping each pair twisted around the other.
4. Using the wire stripper or a penknife, remove approximately 3/8 of an inch of insulation from each of the eight wires. You will have to untwist the wire pairs to accomplish this task, but do not separate the wires in each pair more than 1/2 inch from each other.
5. Using a crimping tool, connect the wires in the RJ-45 connector, matching their color to their correct pin number as described in Table 4-5.

6. Repeat Steps 1 through 5 for the other end of the UTP segment.
7. Use your newly created patch panel to connect your workstation to the network. Can you log on? Can you open a file?
8. If you cannot communicate reliably with the network, try the process again from Step 1. Although you *could* try to remove and reinsert the wires in the connector, this method usually doesn't work. Continue until you can reliably log onto the server from your workstation using your newly made cable.

Project 4-3

As you learned in this chapter, it is sometimes useful to connect two computers directly, rather than go through a traditional network, as you did in the previous exercise. In this exercise you will make a crossover cable and use it to connect two workstations. For this project you will need one workstation running either the Windows 98 or Windows 2000 Professional operating system and one server running the Windows 2000 operating system. Both must contain functioning NICs. You will also need a crimping tool, a wire stripper, a wire cutter, a 5-foot length of CAT5 UTP, and two RJ-45 connectors.

1. On one end of your CAT5 UTP cable, install an RJ-45 connector by following Steps 1–5 of Project 4-2.
2. On the opposite end of the same cable, install an RJ-45 connector in a similar manner, but reverse the locations of the transmit and receive wires. Refer to Figure 4-37 for a visual representation of the crossover cable's RJ-45 terminations.
3. Now that your crossover cable is complete, insert one of the cable's RJ-45 connectors into the workstation's NIC and the other RJ-45 connector into the server's NIC.
4. To test whether your cable works, from the workstation, attempt to view your network connections. To do this from the Windows 98 workstation, double-click the **Network Neighborhood icon**, then double-click the **Entire Network icon** within the Network Neighborhood window. To do this from a Windows 2000 workstation, double-click the **My Network Places icon**, then double-click the **Entire Network icon** in the My Network Places window. Do you see the icon for your server?
5. Now double-click the **server icon** and log on to the server.
6. Once you have logged on, copy a file from your workstation to the server.

Project 4-4

In this exercise, you will have the opportunity to use an atmospheric transmission medium, infrared signaling. Recall that infrared is a line-of-sight medium, meaning that it depends on a direct path between two devices that are trying to communicate.

For this project, you will need a workstation running Windows 98 or Windows 2000 Professional and a printer with an infrared port. Your first step is to make sure that the printer drivers are correctly installed on the workstation.

1. Install and configure drivers for the infrared ports on each device, if they are not already installed.
2. Place the workstation and the printer on the same table, approximately 2 feet apart, with their infrared ports facing each other. Ensure that the workstation recognizes the printer.
3. Print a document using the infrared port.
4. Now turn the printer 180 degrees so that its infrared port faces away from the workstation. Attempt to print the same document. Are you successful?
5. Experiment with moving the devices farther and farther away from each other, while their infrared ports have a direct and clear path between them. At what distance does communication break down?

CASE PROJECTS

1. You have been asked to design the entire cabling system for a medical instrument manufacturer's new central warehouse. The company already has three buildings on two city blocks, and the warehouse will be its fourth building. Currently, the buildings run on separate networks, but the company would like to be able to exchange data among them. In addition, the Marketing Department would like to hold videoconferences with the Sales Department in the next building. In the warehouse, 50 shipping and packing personnel will be riding up and down the aisles on forklifts pulling inventory off the shelves on a daily basis. What kind of transmission media would you recommend for the different departments of the medical instrument company and why?
2. Now the medical instrument company is experiencing data transmission problems in the Quality Control Department, which is located in one corner of the research building. Because only part of a floor is affected, you head for the telecommunications closets in that building. What will you look for?
3. Thanks to your fast thinking, the medical instrument company was able to keep its quality control tasks on track. It has just one more problem: The company has a secret project under way at a warehouse across the street, which is disguised as an antique mall. The project is highly sensitive and its existence cannot be divulged, even to current staff. The medical instrument company executives will not allow any new construction or cabling that might raise suspicion. Nevertheless, they need a way to transmit data to and from the warehouse. What do you suggest?